Projektdokumentation

Einrichten des Webservers der BBS Friedenstraße

Linux Basierend

CentOS 5.8

Sendmail

Projektarbeit F2E2/2012
erstellt von
Marco Gerdes
und
David Goretzky

Erklärung zur selbstständigen Arbeit

Hiermit erklären wir, dass wir die Projektarbeit in
Planung, Installation, Konfiguration und Test der Hardware/Software
selbst durchgeführt und selbstständig erarbeitet haben.

_____	_____
Marco Gerdes	**David Goretzky**

Inhaltsverzeichnis

INHALTSVERZEICHNIS 3

ABBILDUNGSVERZEICHNIS 6

1. BESCHREIBUNG DES PROJEKTES 7
1.1 Vorwort 7
1.2 Aufgabenstellung 8
1.3 Hardware des bestehenden Webservers 9
1.4 Neuer Webserver 9
1.5 Benötigte Software 10
1.6 Arbeitsplatz und benötigte Hardware 10

2. INSTALLATION DER HARDWARE 12
2.1 Vorbereitung zur Inbetriebnahme 12
2.2 Einrichtung der Festplatten 12
2.2.1 Raid 1-Mirroring (Spiegelung) 12
2.2.2 Raid 1 mit Hot - Spare 13
2.2.3 Raid 14
2.2.3.1 Raid 0-Stripping (Beschleunigung ohne Redundanz) 14
2.2.3.2 Raid 10 Leistung und Datensicherheit 15
2.3 Partitionierung der Master / Slave Festplatten 16
2.4 Umsetzung 17

3. INSTALLATION BENÖTIGTER SOFTWARE UND KONFIGURATION 18
3.1 CentOS 18
3.1.1 Installation und Konfiguration 18
3.1.2 Software nachinstalliert nach OS Installation 19
3.2 Webmin 19
3.2.1 Was ist Webmin? 19
3.2.2 Einsatz und Verwendung 19
3.3 DNS 20
3.3.1 Funktionsweise DNS 20
3.3.2 Anordnung der Domains eines DNS 20
3.4 NTP / Hierarchische Struktur 21
3.5 Sendmail 22
3.6 Netzwerk 23
3.7 Avira Mailgate 24
3.7.1 Computerviren 24
3.7.2 Computerwürmer 24
3.7.3 Trojanisches Pferd 24
3.8 Apache HTTP Webserver 25
3.9 MySQL Datenbank-Server 26
3.10 Typo3 27
3.10.1 Verwendung 27
3.10.2 Bedienung 27
3.11 Thunderbird 28
3.12 UPS 29

3.12.1 Ausstattung 30
3.12.2 Betriebsarten einer USV 30
3.12.3 Wartung einer USV 30

4. ADMINISTRATORHANDBUCH 31
4.1 Partitionierung der Festplatten / Raid Konfiguration 31
4.2 Webmin 32
4.3 Netzwerk 33
4.4 NTP 34
4.5 Sendmail 35
4.6 Avira AntiVir MailGate 38
4.7 Apache Webserver 39
4.8 USV 40
4.9 Typo3 40
4.10 Testrechner Konfiguration 41

5. FAZIT 43

6. LITERATURVERZEICHNIS / INTERNETQUELLEN 44
6.1 Foren 44
6.2 Elektronische Nachschlagewerke 44
6.3 Internetquellen, Installations-Informationen und Handbücher 44

7. PROJEKTTAGEBUCH 45
18.01.2012 Mittwoch 45
24.01.2012 Dienstag 45
26.01.2012 Donnerstag 45
01.02.2012 Mittwoch 45
02.02.2012 Donnerstag 45
07.02.2012 Dienstag (08:00 bis 15:00 Uhr) 46
08.02.2012 Mittwoch (08:00 bis 15:00 Uhr) 47
09.02.2012 Donnerstag (11:30 bis 13:05 Uhr) 48
10.02.2012 Freitag (08:00 bis 09:30 Uhr) 48
14.02.2012 Dienstag (08:00 bis 15:00 Uhr) 48
15.02.2012 Mittwoch (08:00 bis 15:00 Uhr) 49
16.02.2012 Donnerstag (11:30 bis 13:05 Uhr) 49
21.02.2012 Dienstag (08:00 bis 15:00 Uhr) 49
22.02.2012 Mittwoch (08:00 bis 15:00 Uhr) 50
23.02.2012 Donnerstag (11:30 bis 13:05 Uhr) 50
28.02.2012 Dienstag (08:00 bis 15:00 Uhr) 50
29.02.2012 Mittwoch (08:00 bis 15:00 Uhr) 51
01.03.2012 Donnerstag (11:30 bis 13:05 Uhr) 51
06.03.2012 Dienstag (08:00 bis 15:00 Uhr) 51
07.03.2012 Mittwoch (08:00 bis 15:00 Uhr) 51
08.03.2012 Donnerstag (11:30 bis 13:05 Uhr) 51
13.03.2012 Dienstag (08:00 bis 15:00 Uhr) 51
14.03.2012 Mittwoch (08:00 bis 15:00 Uhr) 51
15.03.2012 Donnerstag (11:30 bis 13:05 Uhr) 53
20.03.2012 Dienstag (08:00 bis 15:00 Uhr) 53

21.03.2012 Mittwoch (08:00 bis 15:00 Uhr) ... 53
22.03.2012 Donnerstag (09:30 bis 13:30 Uhr) ... 54
28.03.2012 Mittwoch (09:00 bis 15:00 Uhr) ... 55
29.03.2012 Donnerstag (08:30 bis 15:00 Uhr) ... 55
02.04.2012 Montag (09:00 bis 15:00 Uhr) ... 55
03.04.2012 Dienstag (09:00 bis 15:00 Uhr) ... 55
04.04.2012 Mittwoch (09:00 bis 15:00 Uhr) ... 56
12.04.2012 Donnerstag (11:30 bis 13:05 Uhr) ... 57
17.04.2012 Dienstag (08:00 bis 14:55 Uhr) ... 57
18.04.2012 Mittwoch (08:00 bis 14:55 Uhr) ... 58
19.04.2012 Donnerstag (11:30 bis 13:05 Uhr) ... 58
24.04.2012 Dienstag (08:00 bis 14:55 Uhr) ... 58
25.04.2012 Mittwoch (08:00 bis 14:55 Uhr) ... 58
26.04.2012 Donnerstag (11:30 bis 13:05 Uhr) ... 58
02.05.2012 Mittwoch (08:00 bis 14:55 Uhr) ... 59
03.05.2012 Donnerstag (11:30 bis 13:05 Uhr) ... 59
08.05.2012 Dienstag (08:00 bis 14:55 Uhr) Projektende ... 59

8. KONFIGURATIONSDATEIEN ... 60

8.1 /etc/resolv.conf ... 60
8.2 /etc/host.conf ... 60
8.3 /etc/hosts ... 60
8.4 /etc/HOSTNAME ... 60
8.5 /etc/mdadm.conf ... 61
8.6 /etc/apcupsd/apcupsd.conf ... 61
8.7 /etc/avira/avmailgate.conf ... 71
8.8 /etc/avira/avmailgate.acl ... 133
8.9 /etc/avira/groups ... 133
8.10 /etc/avira/avmailgate.ignore ... 134
8.11 /etc/avira/avmailgate-odbc.ini ... 135
8.12 /etc/avira/avmailgate.scan ... 135
8.13 /etc/avira/avmailgate-scanner.conf ... 136
8.14 /etc/avira/avmailgate.warn ... 140
8.15 /etc/avira/avupdate-mailgate.conf ... 141
8.16 /etc/avira/asmailgate.exept ... 143
8.17 /etc/aliases ... 145
8.18 /etc/mail/sendmail.cf ... 149
8.19 /etc/mail/sendmail.mc ... 202
8.20 /etc/httpd/conf/httpd.conf ... 209
8.21 /etc/my.cnf ... 243
8.22 /etc/ntp.conf ... 243

Abbildungsverzeichnis

ABBILDUNG 1- 1: ARBEITSPLATZ GEBÄUDE 60 RAUM 216 10
ABBILDUNG 1- 2: WEBSERVER UND APC-SMART-UPS 700 11
ABBILDUNG 1- 3: TESTRECHNER UND 8-PORT GIGABIT SWITCH 11
ABBILDUNG 1- 4: LAPTOP 1 UND 2 11

ABBILDUNG 2- 1: RAID 1-VERBUND 12
ABBILDUNG 2- 2: RAID 1-VERBUND MIT HOT-SPARE-FESTPLATTE 13
ABBILDUNG 2- 3: RAID 0-VERBUND 14
ABBILDUNG 2- 4: RAID 10-VERBUND 15

ABBILDUNG 3- 1: CENTOS ANFANGSBILDSCHIRM 18
ABBILDUNG 3- 2: DNS STRUKTUR BSP.: WIKIPEDIA 20
ABBILDUNG 3- 3: NTP STRUKTUR 21
ABBILDUNG 3- 4: RECHNERNETZWERKE 23
ABBILDUNG 3- 5: APACHE INDIANER UND LOGO 25
ABBILDUNG 3- 6: MYSQL, PHP, APACHE 26
ABBILDUNG 3- 7: TYPO3 LOGO 27
ABBILDUNG 3- 8: THUNDERBIRD 28
ABBILDUNG 3- 9: APC-SMART UPS 700 29

ABBILDUNG 4- 1: LINUX-RAID KONFIGURATION 31
ABBILDUNG 4- 2: WEBMIN ANMELDEBILDSCHIRM 32
ABBILDUNG 4- 3: SYSTEMINFORMATION 32
ABBILDUNG 4- 4: NETZWERKKONFIGURATION - NETZWERKSCHNITTSTELLEN 33
ABBILDUNG 4- 5: NETZWERKKONFIGURATIONEN - DNS-CLIENT 33
ABBILDUNG 4- 6: NETZWERKKONFIGURATIONEN - HOST-ADRESSEN 34
ABBILDUNG 4- 7: SENDMAIL MAILSERVER - KONFIGURATIONEN 35
ABBILDUNG 4- 8: SENDMAIL MAILSERVER - WEITERLEITUNGSDOMÄNEN 35
ABBILDUNG 4- 9: SENDMAIL MAILSERVER - DOMÄNEN ROUTING 36
ABBILDUNG 4- 10: SENDMAIL MAILSERVER - NETZWERKPORTS 36
ABBILDUNG 4- 11: SENDMAIL MAILSERVER - DOMÄNENMASKIERUNG 37
ABBILDUNG 4- 12: SENDMAIL MAILSERVER - VERTRAUTE BENUTZER 37
ABBILDUNG 4- 13: SENDMAIL MAILSERVER - LOKALE DOMÄNEN 38
ABBILDUNG 4- 14: APACHE-WEBSERVER 39
ABBILDUNG 4- 15: TYPO3 OBERFLÄCHE MIT RICH-TEXT-EDITOR 40
ABBILDUNG 4- 16: BIND DNS-SERVER 41
ABBILDUNG 4- 17: BIND DNS-SERVER MASTERZONE BBS.FH-WILHELMSHAVEN.DE 41
ABBILDUNG 4- 18: BIND DNS-SERVER MASTERZONE TESTWEB.DE 42
ABBILDUNG 4- 19: BIND DNS-SERVER REVERSE-ADRESSE DATENSÄTZE 42

1. Beschreibung des Projektes

1.1 Vorwort

Zum Ende der zweijährigen Fachschule Technik sieht der Lehrplan ein Projekt vor. Das Projekt dient dazu, die während der Ausbildung erlernten Fähigkeiten und Fertigkeiten umzusetzen.

Es gibt mehrere Arten von Projekten. Zum einen gibt es Schulprojekte und zum anderen betriebliche Projekte. Die Projekte umfassen schwerpunktmäßig die Fächer Automatisierungstechnik, Netzwerktechnik und Mikrocontroller.

In der F2E2 2012 werden derzeit 3 SPS-Projekte, ein Projekt Netzwerktechnik und ein kombiniertes Projekt aus Elektronik/Elektrotechnik, Mikrocontroller und Automatisierungstechnik schulisch absolviert und ein Projekt findet in einem Betrieb statt.

Es ist schwierig, ein betriebliches Projekt zu finden, da die meisten Betriebe die Räumlichkeiten oder Personal/Material nicht stellen können. Deshalb findet nur ein Projekt außerhalb statt. Dies beinhaltet Mikrokontroller und Elektronik.

Die Zusammenstellung der Gruppen wurde uns überlassen. Aus gemeinsamen Interessen der einzelnen Klassenmitglieder bildeten sich sehr schnell die Projektgruppen.

Wir entschieden uns für das Projekt Netzwerktechnik. Dies beinhaltet, den derzeitig bestehenden Webserver der BBS Friedenstraße durch einen neuen auszutauschen, die Software auf die heutigen Ansprüche anzupassen und die Projekte der vorangegangen Jahre mit dem Programm Typo3 in die Webseite einzupflegen. Der Webserver dient für den bestehenden E-Mail-Server als Relay für eingehende Mails aus dem Internet. Das setzt voraus, dass Viren, Spam und Dergleichen nicht in das Schulnetz gelangen. Eine dafür vorgesehene Software wird auf diesem Server ebenfalls installiert und konfiguriert.

Zum Ende des Projektes wird nach eingehenden und erfolgreichen Tests der Austausch der Hardware vorgenommen, indem der alte Webserver vom Schulnetz getrennt wird und der neue diese Aufgaben übernimmt.

Diese Dokumentation beschreibt die administrative Konfiguration der Software und die eingesetzte Hardware des dann am Schulnetz betriebenen Webservers.

1.2 Aufgabenstellung

Die Aufgabenstellung zu diesem Projekt war, den derzeitig laufenden Webserver der BBS Friedenstraße durch einen neuen zu ersetzten und die Installation, die Konfiguration, einige Tests und der Austausch der Hard- und Software an diesem vorzunehmen. Hierzu gehören:

- Hardware als Rackserver und APC Smart-UPS vorhanden
- Ermittlung des Ist-Zustandes
- Installation und Tests des Betriebssystems CentOS 6.2 auf einem Software-Raid-1-Verbund
- Integration der UPS Software
- Installation und Test von Webmin zur Remoteadministration
- Installation und Konfiguration des Webservers Apache und des MTA sendmail als Relais zum Mailserver der BBS
- Installation und Konfiguration der Software Avira-Mailgate
- Übernahme der Web-Site (CMS Typo3) und des Techniker-Portals (CMS PragmaMX)
- Datenübertragung der Inhalte aus PragmaMX in Typo3
- Entfernen des obsoleten PragmaMX CMS
- Testen des fertigen Systems
- Austausch des vorhandenen Servers

1.3 Hardware des bestehenden Webservers

Der Webserver relais.bbs.fh-wilhelmshaven.de enthält folgende Hardware:

- Motherboard Tyan S5350 mit 2x CPU Xeon 2800MHz FSB 800
- 1GB ECC PC 333-RAM
- Grafik on Board
- 2x 400 redundantes Netzteil
- LG GSA 4160DVD Brenner
- 2x Maxtor SATA Festplatte 120GB
- 2x GB LAN on Board

1.4 Neuer Webserver

Der neue Webserver relais.bbs.fh-wilhelmshaven.de enthält folgende Hardware:

- SuperServer 6016T-NTRF Model 815-6
  - CPU-Typ: Intel Core i7 / Xeon 3500 / 5500
    - Eigenname: Intel Xeon CPU E5506 @ 2,13 GHz
    - CPU - Takt: 2181,4 MHz (5x 436,3 MHz)
    - CPUs / Kerne: 4
    - L1 - Cache: 16k + 16k, L2 - Cache: 265k, L3 - Cache: 4096k
  - System: Supermicro X8DTU
    - Systemversion: 1234567890
  - Mainboard: Supermicro X8DTU
    - Board - Version: 1234567890
    - Board - S / N: VM14S35399
    - BIOS: AMI
    - Chipsatz: Intel 5520 Tylersburg + Intel ICH10R
    - Speicher: 11776 MB
      - Module: 4096M + 4096M + 4096M + 4096M
    - Schnittstellen: 2x COM, 0x LPT, USB 2.0
    - Grafik: OnBoard Super Micro Computer MAG G200ew WPCM450
    - Super Micro Computer 82576 Gigabit Network Connection
    - Super Micro Computer 82576 Gigabit Network Connection
  - CD / DVD: Optiarc DVD RW AD - 7690H: CD - RW, DVD - RAM, DVD - R DL, DVD+R DL
  - IDE 1: Super Micro Computer ICH10 4 Port SATA DIE Controller
  - IDE 2: Super Micro Computer ICH10 4 Port SATA DIE Controller
  - Festplatten: 2 x 1000GB SATA

1.5 Benötigte Software

Für den neuen Webserver benötigten wir folgende Software:

- CentOS 5.5 (da CentOS 6.2 sich nicht installieren ließ) inklusive aller Updates.
  - CentOS 5.5 wurde mit den Updates auf CentOS 5.8 geupgradet
  - joe
  - yumex
  - php 5.2.17
  - system-config-network
- apcupsd für die APC Smart-UPS 700
- Webmin
  - Apache
  - BindDNS (Laptop für locales Netz)
  - Sendmail
  - MySQL
- Avira Mailgate
- Thunderbird (Testrechner)
- Typo3 (in Verbindung mit Datenbank Übernahme erhalten)

1.6 Arbeitsplatz und benötigte Hardware

Für die Umsetzung des Projektes wurde uns der Raum 216 zur Verfügung gestellt. In diesem Raum war uns die Möglichkeit gegeben, mehrere Netzwerkanschlüsse und Steckdosen zu nutzen, da die UPS, der Test-Rechner, der Webserver und die Laptops einige davon in Anspruch nahmen.

Abbildung 1- 1: Arbeitsplatz Gebäude 60 Raum 216

Die Konfiguration musste im Sinne eines externen Nutzers getestet werden. Hierzu haben wir uns von Herrn Linnemann einen PC zur Verfügung stellen lassen, mit dem wir einmal im lokalen Netz (eigens eingerichtetes privates Netz) den E-Mail-Versand und den Zugriff auf die Webseite testen konnten und das Gleiche aus dem Schulnetz. Des Weiteren diente dieser noch zum Testen der Remoteadministration über Webmin und ssh. Zu dem Test-PC kamen noch zwei Laptops dazu. Der eine Laptop diente für das lokale Netz als DNS Server, damit die Namensauflösung gewährleistet werden konnte, und der zweite Laptop diente ausschließlich für den E-Mail-Versand.

Abbildung 1- 2: Webserver und APC-Smart-UPS 700

Abbildung 1- 3: Testrechner und 8-Port Gigabit Switch

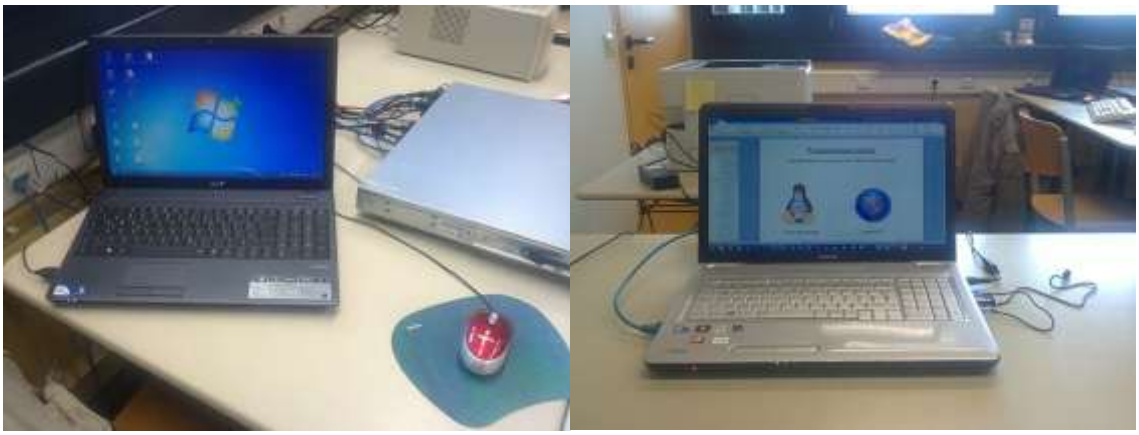


Abbildung 1- 4: Laptop 1 und 2

2. Installation der Hardware

2.1 Vorbereitung zur Inbetriebnahme

Anfänglich haben wir eine Kontrolle durchgeführt, ob die bestellte Hardware vollzählig vorhanden ist. Als dies bestätigt war, begannen wir das vom Werk aus mitgelieferte und eingebaute CD Rom-Laufwerk gegen das mitgelieferte DVD/RW-Laufwerk auszutauschen. Von Herrn Linnemann haben wir uns einen Testrechner, einen Switch, einige Patch Kabel, einen Monitor, zwei Tastaturen und zwei Mäuse geben lassen. Die Smart-UPS hat Herr Appenzeller besorgt, inklusive des seriellen Verbindungskabels von der UPS zum Webserver. Die Hardware ist jetzt soweit vorbereitet und wurde in Betrieb genommen.

2.2 Einrichtung der Festplatten

Die Einrichtung der Festplatten sieht vor, dass die vorhandenen SATA-Festplatten mit je 1000GB in einem Raid 1-Verbund laufen. Da es uns von der vorhandenen Hardware her nicht gegeben war einen Raid 1-Verbund mit Hot-Spare Festplatte einzurichten, entschieden wir uns unter Absprache mit der Projektleitung, einen Raid 1-Verbund ohne Hot-Spare einzurichten.

2.2.1 Raid 1-Mirroring (Spiegelung)

RAID 1 ist der Verbund von mindestens zwei Festplatten. Ein RAID 1 speichert auf allen Festplatten die gleichen Daten (Spiegelung) und bietet somit volle Redundanz. Die Kapazität des Arrays ist hierbei höchstens so groß wie die kleinste beteiligte Festplatte.

Der eingerichtete Raid 1-Verbund sieht wie folgt aus:

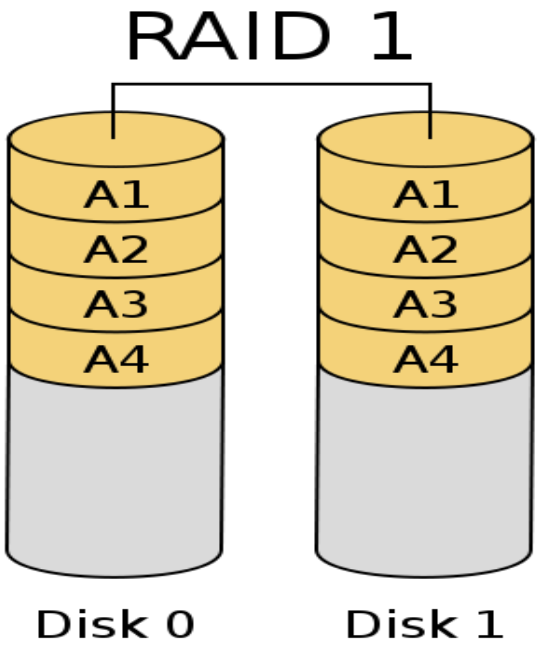


Abbildung 2- 1: Raid 1-Verbund

2.2.2 Raid 1 mit Hot - Spare

Dieser Verbund besteht aus einer Master-, einer Slave- und einer Hot-Spare-Festplatte. So wie beim Raid 1-Verbund wird hier die Master-Festplatte (Disk 0) auf die Slave-Festplatte (Disk 1) gespiegelt. Das Besondere in diesem Verbund ist, sollte mal eine Festplatte ausfallen, egal welche, so übernimmt sofort die Hot-Spare-Festplatte. Sie spiegelt dann die Daten von der noch laufenden Festplatte und übernimmt die Stelle der ausgefallenen. Somit ist immer gewährleistet, dass ein Raid 1-Verbund besteht und man die ausgefallene Festplatte ohne Systemausfall tauschen kann.

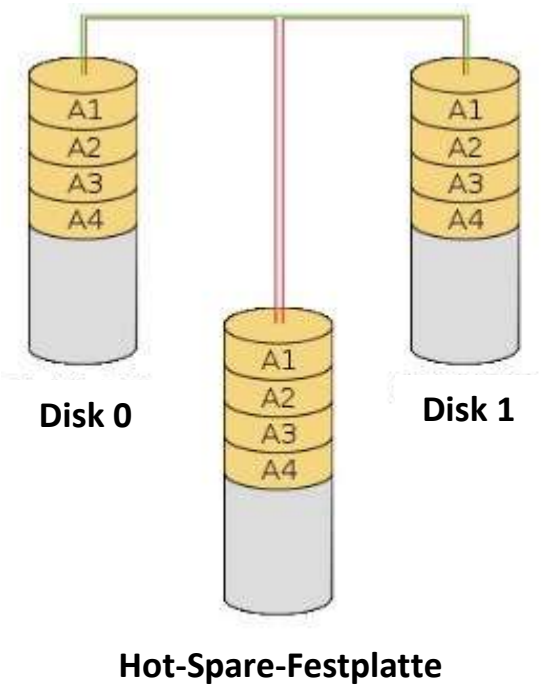


Abbildung 2- 2: Raid 1-Verbund mit Hot-Spare-Festplatte

2.2.3 Raid

Definition: Der Begriff Raid kommt aus dem Englischen und bedeutet „Redundant Array of Independent Disk“. Übersetzt bedeutet dies „Redundante Anordnung unabhängiger Festplatten“.

Ein Raid-Verbund fasst mehrere physische Laufwerke zu einem logischen Laufwerk zusammen. Daraus resultiert eine wesentlich höhere Datensicherheit, denn es werden gezielt doppelte Daten erzeugt. Bei Ausfall eines Laufwerks besteht noch ein zweites, das die identischen Daten des defekten Laufwerks hat und somit eine Ausfallsicherheit gewährleistet. Daraus resultiert, dass das defekte Laufwerk im laufenden Betrieb getauscht werden kann, ohne dass es zu Datenverlusten kommt. Es gibt die unterschiedlichsten Arten von Raid-Verbunden. Am geläufigsten sind Raid 1, wie bei unserem Webserver verwendet (Punkt 2.2.1), Raid 0 und Raid 10.

2.2.3.1 Raid 0-Stripping (Beschleunigung ohne Redundanz)

Diese Art von Raid gehört genau genommen nicht zu den Raid Systemen, da die Redundanzen fehlen. Es ist ein „Array of Independent Disks“. Diese Art des physikalischen Laufwerk Verbunds bietet hohe Transferraten, indem die beteiligten Festplatten in zusammenhängende Blöcke gleicher Größe aufgeteilt werden. Der Zugriff auf die Platten erfolgt parallel (engl. Stripping = in Streifen zerlegen). Die Größe der Datenblöcke wird als Stripping-Granularität (auch stripe size, chunk size oder interlace size) bezeichnet. Bei Raid 0 wird meist eine chunk size von 64 kB gewählt. Fällt eine Festplatte vollständig aus, so sind die Daten bei geringer Stripping Granularität wiederherstellbar. Dies geht jedoch nur bei kleinen Datenmengen, meist sind die Daten dann unwiderruflich verloren.

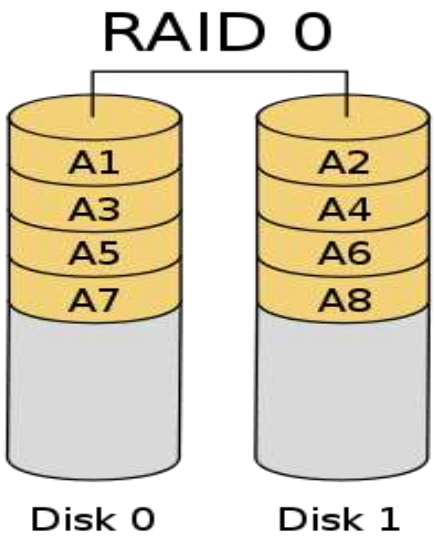


Abbildung 2- 3: Raid 0-Verbund

2.2.3.2 Raid 10 Leistung und Datensicherheit

Ein Raid 10 Verbund sind mehrere Raid 1 Verbunde (mindestens 2), Verbunden über ein Raid 0. Es kombiniert die Eigenschaften eines Raid 0 und Raid 1 Verbundes. Sicherheit und gesteigerte Schreib-/Lesegeschwindigkeit. Dieser Raid Verbund benötigt mindestens vier Festplatten. Bei Ausfall einer Festplatte ist eine schnelle Datenrekonstruktion möglich, da nur ein Teil der Daten rekonstruiert werden muss.

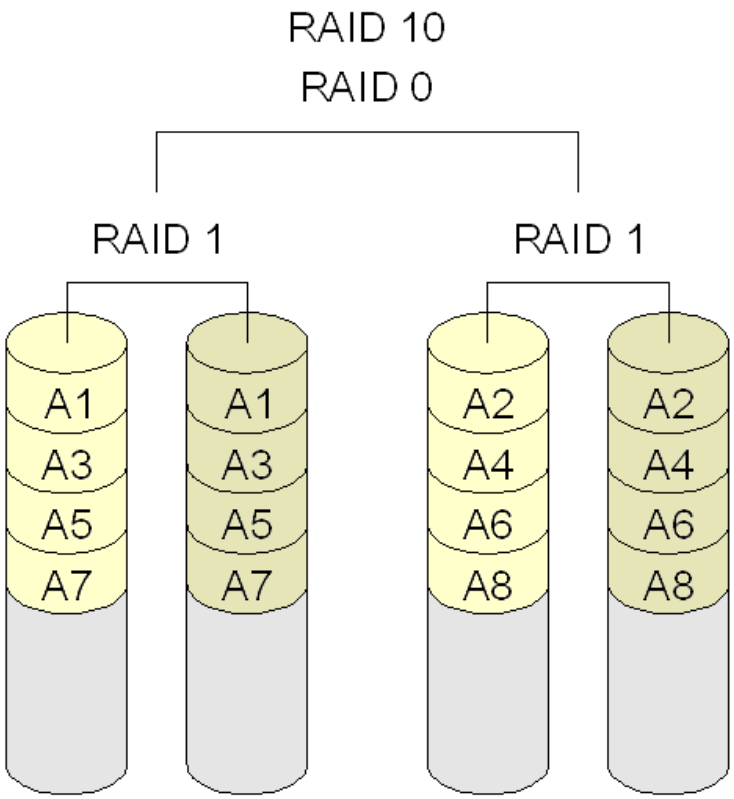


Abbildung 2- 4: Raid 10-Verbund

2.3 Partitionierung der Master / Slave Festplatten

Unter einer Partition (lat. Partitio = „(Ein)teilung“) versteht man einen zusammenhängenden Teil des Speicherplatzes eines geeigneten physischen oder logischen Datenträgers. Die Partitionierung eines solchen, bzw. mehrerer Datenträger, ist sehr wichtig, da dies einen großen Einfluss auf die Performance eines Rechners hat.

Wir haben die Master / Slave Festplatten in jeweils vier Partitionen aufgeteilt.

Die erste Partition ist die boot Partition (md0 /boot = sda1, sdb1).

- In der boot Partition befindet sich der Verweis wo beim Startvorgang die Kernel-Dateien zu finden sind. Des Weiteren befindet sich in dieser noch der GRUB. Der GRUB ist der sogenannte Bootloader. Er bekommt vom BIOS die Kontrolle zum Booten übergeben. Im Grub stehen alle nötigen Systemeinträge und Verweise, die zum Starten notwendig sind.

Die zweite Partition ist die Swap-Partition (swap = sda2, sdb2).

- Diese Partition ist die Pufferpartition für das RAM. Die im Moment nicht benötigten Daten des RAMs werden in die Swap-Partition ausgelagert.

Die dritte Partition ist die Root-Partition (md1 / = sda3, sdb3).

- Die Root-Partition ist die wohl wichtigste Partition in einem Linux System. Sie wird mit dem Zeichen / gekennzeichnet und ist die Wurzel aller anderen Verzeichnisse. Sie enthält außerdem die zum Booten unbedingt erforderlichen Kerneldateien.

Die vierte Partition ist die erweiterte Partition (erweiterte Partition = sda4, sdb4).

- Da auf einer Festplatte nur 4 primäre Partitionen möglich sind, ist eine erweiterte Partition nötig, um mehr als 4 Partitionen erstellen zu können.

Die fünfte Partition ist die Options-Parsing-Tool-shared-library-Partition
(md 2 /opt = sda5, sdb5).

- Auf dieser Partition werden alle übrigen Programme installiert. Diese war für uns nur zur Datenbankübernahme (Typo3) wichtig, da wir dort die Daten zwischengespeichert haben.

2.4 Umsetzung

Als die Hardware soweit eingerichtet war, haben wir begonnen die Software zu installieren. Die Vorgabe für unser Projekt war die Systeminstallation von CentOS 6.2.

Dies erwies sich als sehr problematisch, da diese Version von CentOS mit den vorkonfigurierten Festplatten, auf einem Hardware-Raid, nicht installiert werden konnte. Wir mussten dann mit Hilfe einer LinuxLiveCD die Festplatten-Partitionierung vornehmen und die Vorkonfiguration entfernen.

Die Installation konnte nun mit Erfolg beendet werden, aber nun gab es ein neues Problem. Die geläufigsten Programme, wie der Texteditor joe oder das graphische Installationstool yumex, konnten nicht bzw. nur schwer installiert werden.

Nach Rücksprache mit der Projektleitung unter Zugrundlegung des Für und Wider kamen wir zu dem Ergebnis, dass wir diese Version gegen die CentOS 5.5 tauschen.

Die neue Installation verlief ohne Probleme und die Neu-Partitionierung der Festplatten konnte direkt im Installationsverlauf vorgenommen werden. Nach der erforderlichen Installation der notwendigen Grundprogramme (joe, yumex, Netzwerkmanager, sendmail, …) wurden noch die Master und Slave Festplatte bootfähig gemacht und die Hardwaretests durchgeführt.

Als es dann soweit war, das OS lief und Updates wurden regelmäßig bezogen, kamen wir zur Installation von Sendmail und dem Avira-MailGate. Die nächsten Probleme folgten auf den Fuß.

Für die sendmail-Konfiguration haben wir mehr als sechs Anläufe gebraucht, da die Einrichtung des Programms, unter Berücksichtigung der Standortbedingung sich als äußerst schwierig erwiesen hat. Doch auch dies fand ein Ende, nachdem lokal und öffentlich alles funktionierte.

Als Nächstes kam die Konfiguration von AV-Mailgate, nachdem wir feststellen mussten, dass der aktive, derzeit betriebene, Webserver keinen Viren- und Spamschutz hat. Wir hatten uns unter Rücksprache mit Herrn Linnemann geeinigt, dass wir die Konfiguration vorerst beibehalten, um den IST-Zustand der aktiven Anlage zu erfüllen. Die Installation des Programms erfolgte, bevor der neue Lizenzschlüssel (hbedv.key) erschienen war. Dieser kam nach einiger Zeit dann auch, doch wir merkten, dass der Schlüssel nur bei der Installation mit übernommen werden kann und somit installierten und konfigurierten wir nochmals neu.

Bei genauerem Hinsehen war auch ersichtlich, warum der aktive Webserver keinen Spam-Schutz hat. Hierfür wird von der Firma Avira ein eigens dafür vorgesehener Schlüssel verkauft. Deshalb entschieden wir uns, nach Absprache mit Herrn Linnemann, den Spam-Schutz deaktiviert zu lassen.

Für die Übernahme der Webseite mussten wir noch einige Veränderungen bzw. Versionsaktualisierungen vornehmen, denn, wie sich herausstellte, hat Typo3 die Eigenart, bei einer bestehenden Webseite immer die gleiche php und mysql Version zu nutzen.

Nach der Aktualisierung war die Übernahme relativ einfach. Danach haben noch die Ordnerstrukturen angepasst und die Webseite überarbeitet. Nach eingehender Überlegung mit Herrn Gerdes und Herrn Appenzeller kamen wir zu dem Schluss, dass es am sinnvollsten sei, die aktive Webseite auf dem laufenden Webserver zu bearbeiten und diese dann mit dem neuen Webserver zu synchronisieren.
Nach der Synchronisierung erfolgte ein letzter Check und die Programme wurden untereinander angepasst.

Die Einsatzbereitschaft des Webservers ist gewährleistet.

3. Installation benötigter Software und Konfiguration

3.1 CentOS

CentOS ist ein Gemeinschaftsprojekt, das ein zu Red Hat Enterprise Linux (RHEL) kompatibles System zur freien Nutzung bereitstellt.

Abbildung 3- 1: CentOS Anfangsbildschirm

3.1.1 Installation und Konfiguration

Bei der Installation haben wir wie in Punkt 2.3 die Partitionierung der Festplatten vorgenommen und die benötigten Serverdienste installiert. Das OS wird graphisch über den KDE Desktop administriert.

3.1.2 Software nachinstalliert nach OS Installation

Nach der Installation haben wir noch den Text-Editor joe, das graphische Installations-Tool Yumex, Sendmail, Netzwerk-Konfigurations-Tool, APC UPS Software, Webmin und AV-Mailgate installiert. Näheres hierzu folgt auf den nächsten Seiten.

3.2 Webmin

3.2.1 Was ist Webmin?

Webmin ist ein browserbasierendes Administrationstool, welches es ermöglicht, Linux-Server-Systeme vom Arbeitsplatz aus zu betreuen. Dieses Open-Source-Tool wird mit plattformunabhängiger Software betrieben, die nahezu auf jedem Rechner zu finden ist. Einem Webbrowser zum Beispiel. Dieses Tool ist vielseitig konfigurierbar und besitzt sogar seinen eigenen Webserver für die Anzeige im Browser.

Es ist modular aufgebaut und unterstützt fast jede wichtige Komponente auf Linux-Rechnern. Webmin stellt beispielsweise eine Schnittstelle bereit für Apache-, Samba-, Datenbank-, Firewall-, Hardware-, Cronjobs- oder Backup-Konfigurationen. Der Zugriff auf die Konsole ist verschlüsselt, über ein eingebautes Java-Applet, möglich. Webmin ist fast komplett in Perl geschrieben, somit ist gewährleistet, dass es auf jeder gängigen Linux-Distribution läuft.

3.2.2 Einsatz und Verwendung

Webmin findet meist dort Verwendung, wo Unix/Linux Serversysteme laufen und die Administratoren mehrere Server betreuen müssen. Natürlich wird Webmin auch dort verwendet, wo nur ein Server betrieben wird. Doch meist erfolgt die Administration dann direkt am Server über die Konsole.
Bei unserem Projekt Webserver nutzen wir Webmin, um die Administration von Sendmail, Apache, Bind DNS (Testrechner), MySQL und des Netzwerkes durchzuführen.

3.3 DNS

Das Domain Name System / Server (DNS) ist einer der wichtigsten Dienste im Netzwerk. Er ist zuständig, Anfragen zu beantworten, die die Namensauflösung betreffen.

3.3.1 Funktionsweise DNS

Den DNS muss man sich wie ein riesiges Adressbuch vorstellen. Hier kommen die Anfragen an, die man über die Adressleiste der verschiedenen Internetbrowser eingeben kann. Eine spezielle Software sucht aus der Datenbank das Feld heraus, welches mit der eingegebenen Adresse übereinstimmt. In einer weiteren Zelle der Datenbank ist die IP Adresse des Servers hinterlegt, auf dem die Daten gespeichert sind, die auf der jeweiligen Webseite angezeigt werden sollen. Über die IP Adresse, die aus Zahlenkombinationen besteht, wird die Suchanfrage an die entsprechende Stelle weitergeleitet.

3.3.2 Anordnung der Domains eines DNS

Ähnlich wie beim Ordnungssystem der Dateien in Windows kommt es anschließend zur Gliederung in Hauptdomains, die dann wiederum in die Subdomains bis hin zu den einzelnen in einer Subdomain vorhandenen Unterseiten aufgelöst werden. Dabei dürfen in den Domainnamen, die in der kompletten Hierarchie auch URL genannt werden, keine Sonderzeichen außer einem Punkt oder einem Bindestrich vorkommen. Dieses liegt daran, dass alle anderen Sonderzeichen nicht in eine international anwendbare, maschinentaugliche Sprache übersetzt werden können. Dieser Fakt trifft vor allem auf die in einigen Sprachen üblichen Umlaute und besonderen Vokalzeichen zu.

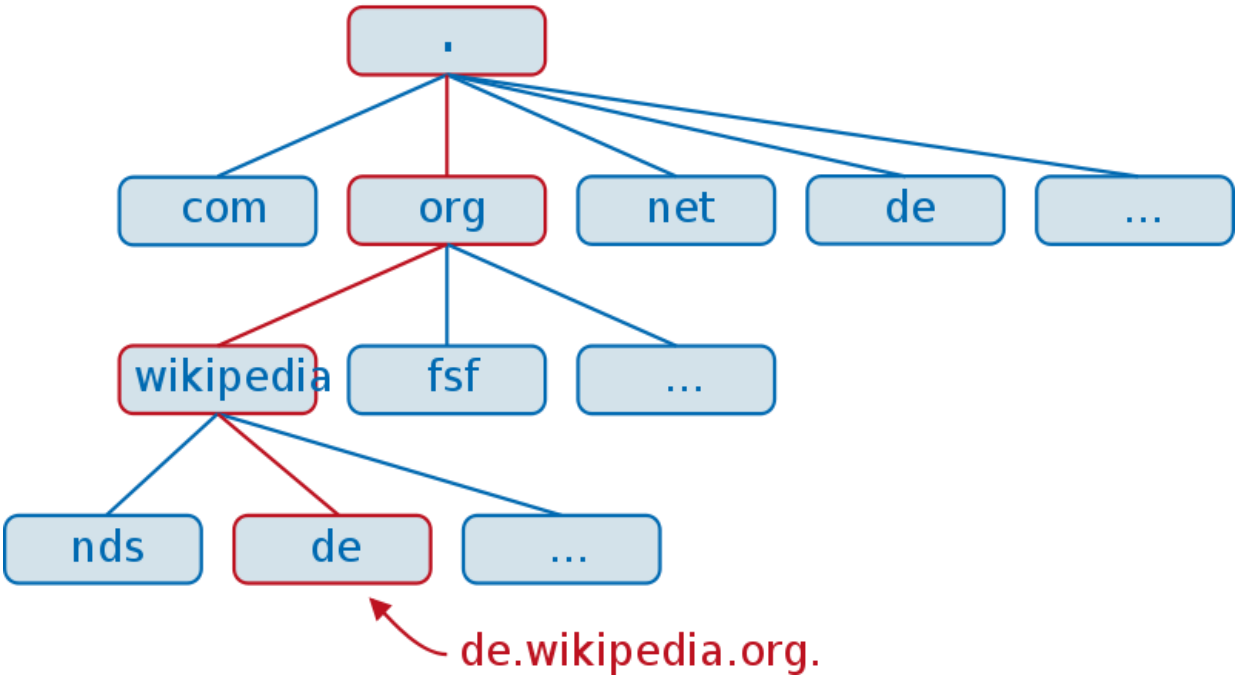


Abbildung 3- 2: DNS Struktur Bsp.: Wikipedia

3.4 NTP / Hierarchische Struktur

Zu der Synchronisierung von Systemuhren in Computersystemen wird das Network-Time-Protocol (NTP) verwendet. Dies ist ein Standard und wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke, mit variabler Paketlaufzeit, zu ermöglichen. Dieses Protokoll verwendet das verbindungslose User-Datagramm-Protocol (UDP).

Beim NTP gibt es eine hierarchische Struktur. Diese Struktur setzt sich aus verschiedenen Strata zusammen. Die hier zu sehenden Uhren werden als Stratum 0 bezeichnet. Dieses Stratum ist das sogenannte Zeitnormal, wie z.B. eine Atomuhr. Die nachfolgenden Strata 1 - 3 ordnen sich, der Reihenfolge nach, unter. Ein Strata ist der Client des darüber liegenden, aber auch zugleich der Server des darunterliegenden.

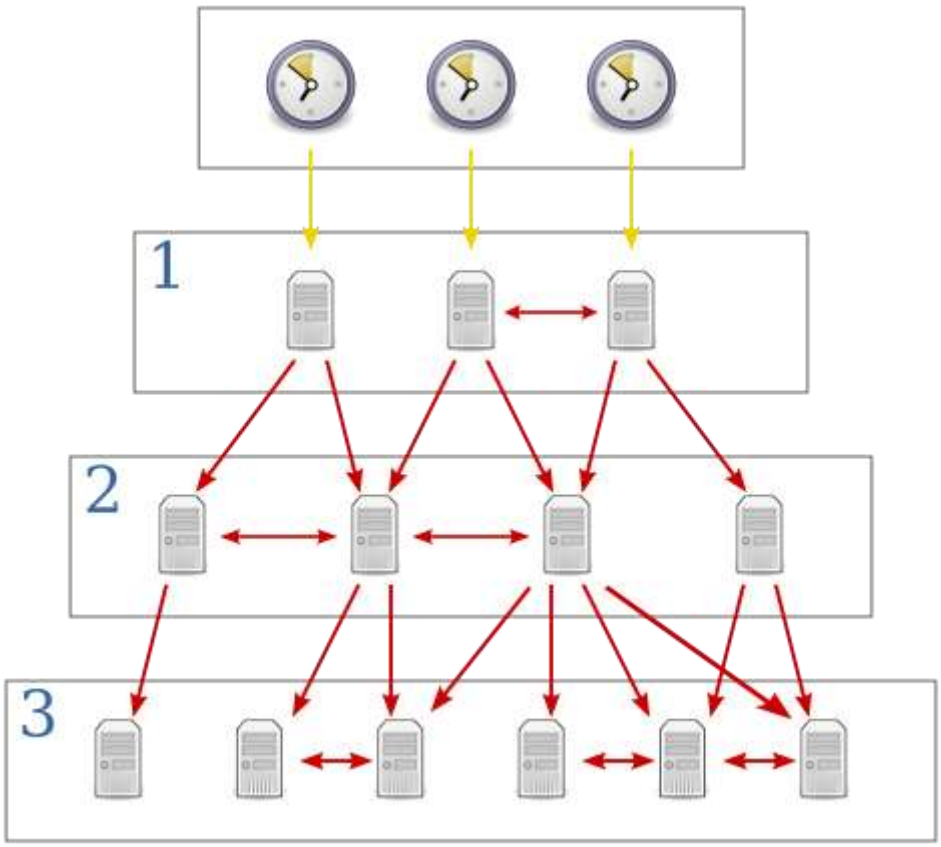
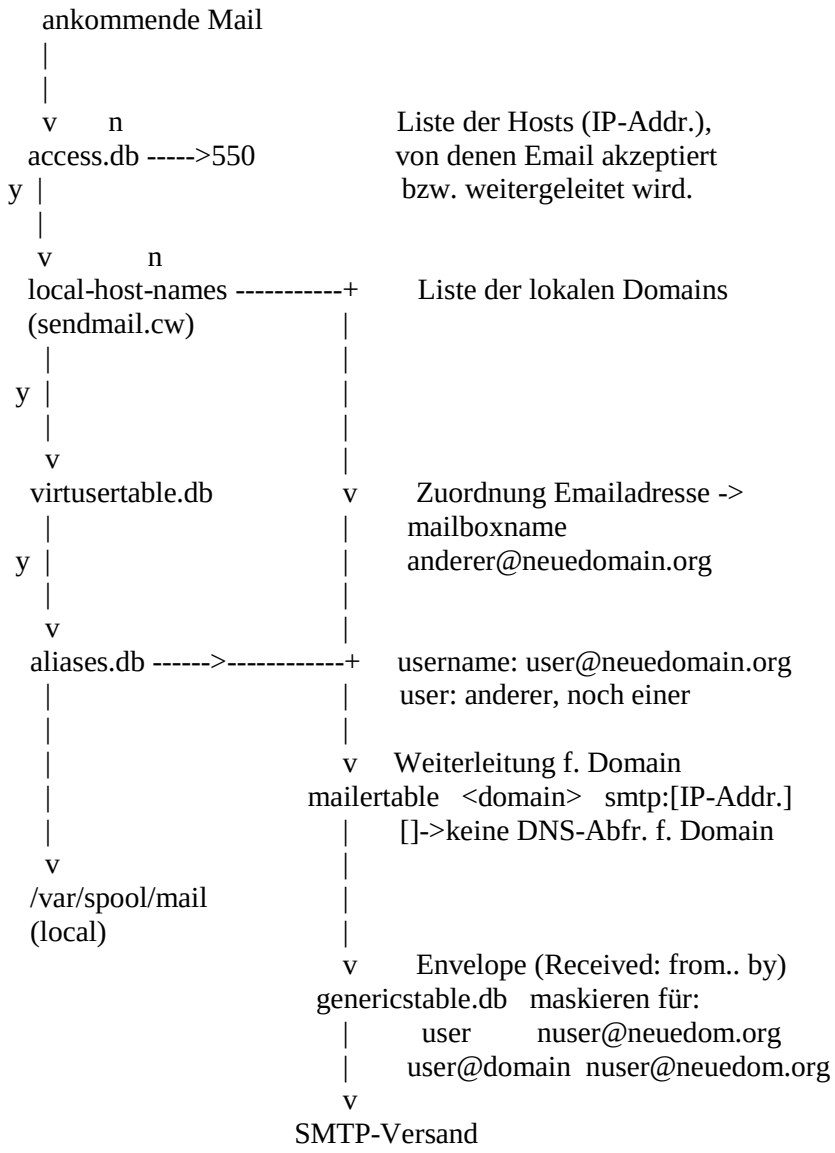


Abbildung 3- 3: NTP Struktur

3.5 Sendmail

Sendmail ist ein Mail Transfer Agent (MTA). Dieses Programm hat sehr weite Verbreitung gefunden, so dass viele Unix Programme davon ausgehen, Sendmail installiert und konfiguriert vorzufinden. Sendmail an sich ist sehr schwer zu konfigurieren, da es sehr komplex ist. In Fachkreisen sagt man auch: „Wer ein richtiger Administrator ist, hat schon mindestens einmal eine m4.conf bzw. eine sendmail.cf per Hand konfiguriert“. Wenn eine E-Mail von Sendmail verschickt wird, durchlaufen die Headerinformationen verschiedene Tests durch die einzelnen Konfigurationsdateien. Nachfolgend ist der Datenfluss durch Sendmail aufgeführt.



3.6 Netzwerk

Als Netzwerk wird der Zusammenschluss mehrerer Rechner bezeichnet, die man mit Datenleitungen miteinander verbunden hat. Die Kommunikation erfolgt über Dienstprogramme und Protokolle. Die Verwaltung, Verteilung und zum Teil die Sicherheit des Netzwerkes übernehmen Server. Man unterscheidet zwischen lokalen Netzwerken, wie beispielsweise einem Schulnetzwerk oder einem Firmennetzwerk, und externen Netzwerken. Solche sind beispielsweise VPN-Verbindungen zwischen Firma und externen Mitarbeitern oder das Internet selbst. Die Konfiguration des jeweiligen Netzwerkes kann grafisch erfolgen, über diverse Tools, die standartmäßig auf allen Betriebssystemen vorhanden ist, aber auch über Terminal und Konsolenbefehle. Für administrative Zwecke ist es geläufig, browserbasierende Webadministrationstools zu nutzen, da man die Administration bei entsprechender Konfiguration auch aus der Ferne vornehmen kann. In unserem Fall übernahm diese Aufgabe das Admin-Tool Webmin.

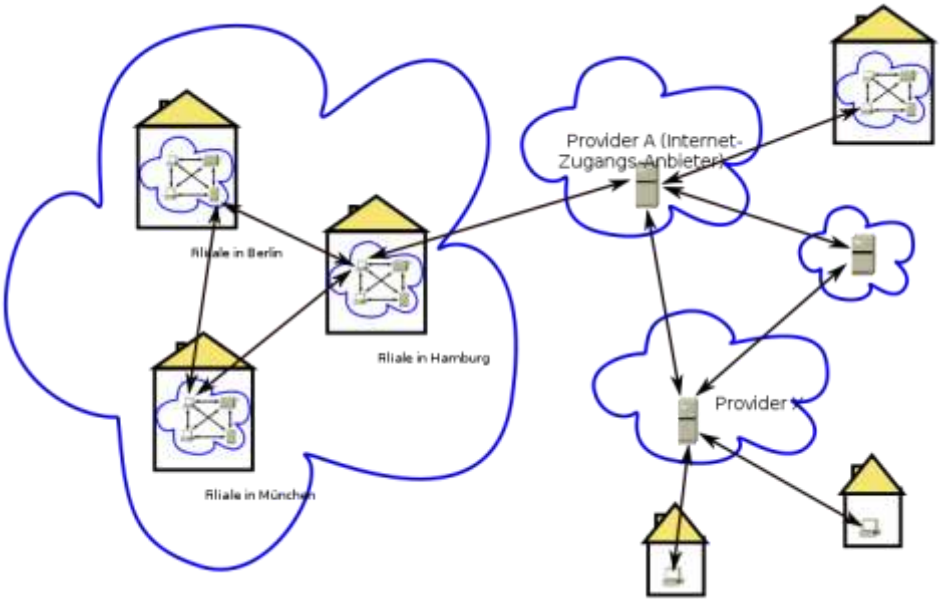


Abbildung 3- 4: Rechnernetzwerke

3.7 Avira Mailgate

AvMailgate ist ein sehr umfassendes und für den E-Mail Verkehr nicht mehr wegzudenkendes Programm. Dieses Programm bietet einen umfassenden Schutz für ein - und ausgehende E-Mails in Echtzeit. Es kontrolliert Anhänge einer E-Mail auch in komprimierter Form, verschiebt automatisch unbekannte, infizierte oder verdächtige Dateien in Quarantäne. Erkennung von Makroviren und Überprüfung von verschlüsselten E-Mails beinhaltet es ebenfalls. Bei diesem Programm ist so gut wie alles enthalten, was man benötigt um einen sicheren und sauberen Versand von Emails zu gewährleisten.

3.7.1 Computerviren

Ein Computervirus ist ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsgefahr wie bei seinem biologischen Pondon.

3.7.2 Computerwürmer

Ein Computerwurm ist ein Programm oder ein Skript mit der Eigenschaft, sich selbst zu vervielfältigen, nachdem es ausgeführt wurde. Im Gegensatz zum Computervirus verbreitet sich der Computerwurm, ohne fremde Dateien oder Bootsektoren mit seinem Code zu infizieren.

3.7.3 Trojanisches Pferd

Ein in der EDV bezeichneter Trojaner ist ein Programm, was als nützliche Anwendung getarnt ist, aber im Hintergrund ohne Wissen des Anwenders eine andere Funktion erfüllt.

Diese hier aufgeführten Punkte werden umgangssprachlich als Computerviren bezeichnet, sind aber klar davon abzugrenzen, bis auf das Computervirus. Sie fallen alle drei unter die Kategorie Schadsoftware oder werden auch Malware genannt.

3.8 Apache HTTP Webserver

Der Apache HTTP Webserver ist einer der meistbenutzten Webserver im Internet. Er ist als Open Source Software zu beziehen, da er ein quelloffenes und freies Produkt der Apache Software Foundation ist. Er unterstützt neben Unix und Linux auch Win32, NetWare sowie eine Vielzahl weiterer Betriebssysteme. In der Weiterentwicklung wurden beispielsweise die Apache Portable Runtime (ARP) Bibliothek für die Betriebssysteme Optimiert. Der Aufbau des Apache HTTP Webserver ist modular aufgebaut. Durch entsprechende Module kann er beispielsweise die Kommunikation zwischen Browser und Webserver verschlüsseln (mod_ssl), als Proxyserver eingesetzt werden (mod_proxy) oder komplexe Manipulation von HTTP-Kopfdaten (mod headers) und URLs (mod_rewrite) durchführen. Durch serverseitige Skriptsprachen bietet er die Möglichkeit, Webseiten dynamisch zu erstellen. Die geläufigsten Skriptsprachen sind PHP, Perl und Ruby. Diese sind jedoch nicht Bestandteil des Webservers, sondern müssen entweder als Modul eingebunden werden oder über das CGI angesprochen werden. Das Server Side Includes (SSI) kann mit dem bei der Installation enthaltene mod_include ausgeführt werden. Dies ermöglicht einfache dynamische Webseiten zu erstellen und den Verwaltungsaufwand von statischen Webseiten zu minimieren.

Abbildung 3- 5: Apache Logo

3.9 MySQL Datenbank-Server

MySQL ist das weltweit am meisten verbreitete relationale Datenbankverwaltungssystem. Es ist ebenfalls eine Open-Source-Software und bildet die Grundlage für viele dynamische Webauftritte. Ein bevorzugtes Einsatzgebiet ist Datenspeicherung für Webservices. MySQL wird dabei häufig in Verbindung mit dem Webserver Apache und der Skriptsprache PHP eingesetzt, wie es bei dem Webserver der BBS-Friedenstraße ebenfalls der Fall ist. MySQL mit PHP wird in unseren Fall verwendet, um Daten auf der Webseite http://www.bbs.fh-wilhelmshaven.de bereitzustellen. Diese Webseite wurde mit der Open Source Software Typo 3 erstellt. Dieses Programm erfordert MySQL, damit eine Dynamisierung der Webseite möglich ist. Apache ist dafür zuständig, diese Webseite im World Wide Web bereitzustellen. Da sich regelmäßig beispielsweise das Essensangebot im Bistro oder das Angebot an Praktikumsplätzen ändert, ist es sinnvoll, jeweils eine Datenbank pro Informationsquelle zu betreiben. So wird gewährleistet, dass Aktualisierungen ohne hohen Zeit- und Kostenaufwand bereitgestellt werden können und die Webseite dauerhaft online ist.

Abbildung 3- 6: MySQL, PHP, Apache

3.10 Typo3

Typo3 ist ein freies Content-Management-Framework für Websites, das ursprünglich von Kasper Skårhøj entwickelt wurde. Typo3 basiert ebenfalls auf der Skriptsprache PHP. Datenbanken für Typo3 können MySQL, PostgreSQL oder Oracle sein.

3.10.1 Verwendung

Weltweit werden schätzungsweise mehr als 500.000 Webserver damit betrieben. Typo3 stellt eine mittlere Anforderung an die Leistungs- und Konfigurationsfähigkeit des verwendeten Servers. Voraussetzungen für einen Webseiten Betreuer ist eine intensive Befassung mit der Metasprache TypoScript.

3.10.2 Bedienung

Typo3 wird auf einem Webserver installiert und mit einem Webbrowser benutzt. Außer einem Browser ist zur Bedienung keine Zusatzsoftware erforderlich. Die Nutzung von Typo3 gliedert sich in drei große Bereiche. Die Erstellung des Website-Designs, die Konfiguration von Typo3 mittels TypoScript und die Eingabe des Website-Inhalts. Typo3 enthält ein Backend, das der Pflege der Website dient und ein Frontend, das die Website selbst darstellt.

Abbildung 3- 7: Typo3 Logo

3.11 Thunderbird

Mozilla Thunderbird ist ein freies Open-Source-E-Mail-Programm und Newsreader des Mozilla-Projekts. Das Programm basiert auf dem Quelltext der Mozilla Suite und ist unter anderem für Windows, Linux, Mac OS X, BSD, Solaris, eComStation und OS/2 verfügbar. Es ist neben Microsoft Outlook eines der am weitesten verbreiteten Programme zum Lesen von News und E-Mails. In dem Programm ist ein lernfähiger Spamfilter integriert und es unterstützt Imap und POP3.

Abbildung 3- 8: Thunderbird

3.12 UPS

UPS bedeutet Uninterruptible Power Supply. Der Einsatz erfolgt an Systemen, auf denen empfindliche Daten gespeichert sind, die bei Schwankungen im Stromnetz vor Absturz oder gar Verlust geschützt werden müssen. USV-Geräte finden daher vor allem in Krankenhäusern, Leitstellen, modernen Eisenbahn-Stellwerken und Rechenzentren Verwendung, mittlerweile aber ebenso in kleinen Büros (SoHo) oder zu Hause. Sie werden in Stromzuleitungen der zu sichernden Anlagen oder Geräten eingefügt. Sie kann die Stromversorgung für einen kurzen Zeitraum gewährleisten, so dass beispielsweise Rechner kontrolliert, über eine spezielle Software, heruntergefahren werden können.

Abbildung 3- 9: APC-Smart UPS 700

3.12.1 Ausstattung

Die Ausstattung einer USV ist leicht überschaubar. Sie besteht lediglich aus den Akkus, den Stromrichtern, einer elektronischen Steuerung und der elektronischen Regelung.

3.12.2 Betriebsarten einer USV

Die Verbindung zwischen einer USV und dem entsprechendem Rechner wird standardmäßig über Ethernet oder SNMP (Simple Network Management Protocol) hergestellt. Vereinzelt kann diese Verbindung auch über eine RS-232 Schnittstelle oder über USB erfolgen. Durch diese Kommunikation zwischen den Geräten kann die USV auch überwacht, gesteuert und eingestellt werden.
Durch die Konfiguration einer USV können die Rechner bei Stromausfall automatisch heruntergefahren werden. Somit werden wichtige Dateien oder Programmabläufe nochmals gespeichert bzw. beendet. Durch diesen Prozess wird sowohl die Software als auch die Hardware vor Schäden bewahrt.
In größeren Rechenzentren werden meistens Notstromgeneratoren eingebaut. Durch diesen Zusatz brauchen die USV-Geräte nur noch die Zeit zu überbrücken, bis die Generatoren auf Nennleistung angelaufen sind. Ab diesen Zeitpunkt übernehmen diese wieder die Stromversorgung des Netzes.

3.12.3 Wartung einer USV

Die Wartung einer USV sollte für einen reibungslosen und stets sicheren Ablauf regelmäßig durchgeführt werden. Eine Selbstwartung ist zum Teil in den USVs schon mit eingebaut. Sie besteht darin, dass in regelmäßigen Abständen die Akkus im laufenden Betrieb mit angeschlossener Last entladen werden. Zusätzlich sollte man aber auch die Akkus an sich nicht außer Acht lassen. Bei 10-Jahres-Batterien sollten die Akkus spätestens nach acht Jahren und bei 5-Jahres-Batterien nach spätestens vier Jahren komplett gewechselt werden. Dies beugt einem Ausfall der Anlage durch defekte Akkus vor.

4. Administratorhandbuch

4.1 Partitionierung der Festplatten / Raid Konfiguration

Während der Installation von CentOS haben wir die Festplatten partitioniert und im Raid 1-Verbund zusammengefügt.

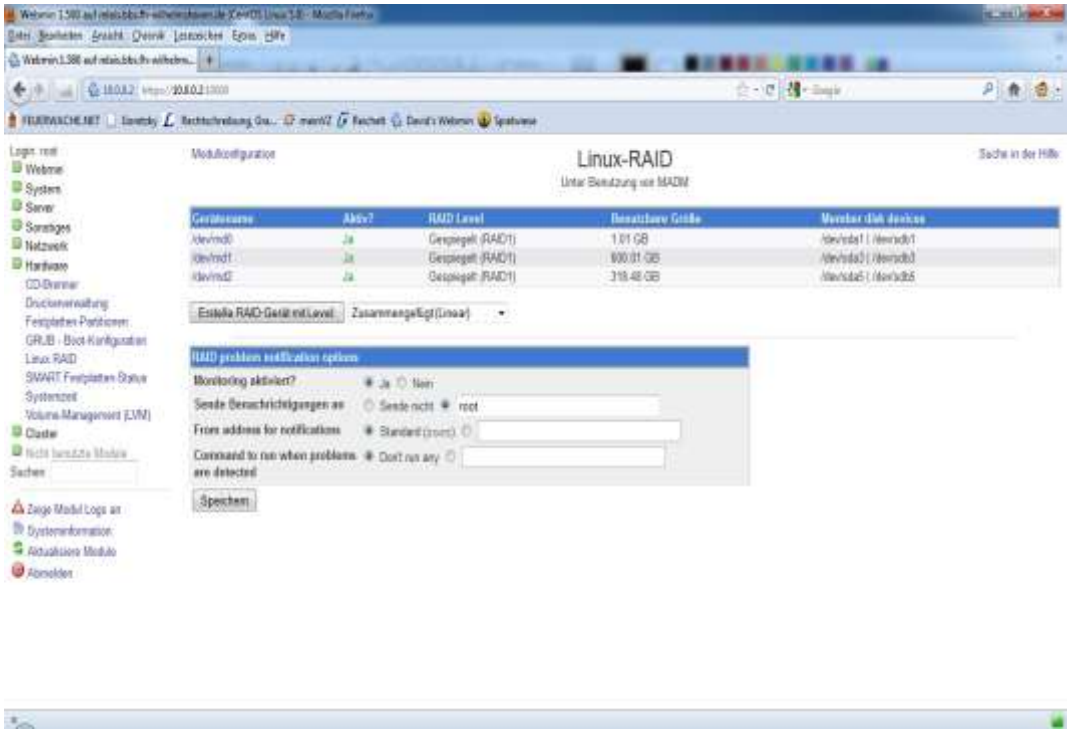


Abbildung 4- 1: Linux-RAID Konfiguration

4.2 Webmin

Nach dem Download der aktuellen Webmin Version 1.580 haben wir diese mit dem Befehl yum localinstall --nogpgcheck webmin-1.580-1.noarch.rpm installiert.
Danach kommt man mit einem beliebigen Browser und der Adresse https://127.0.0.1:10000 auf die Webmin Anmeldeseite.

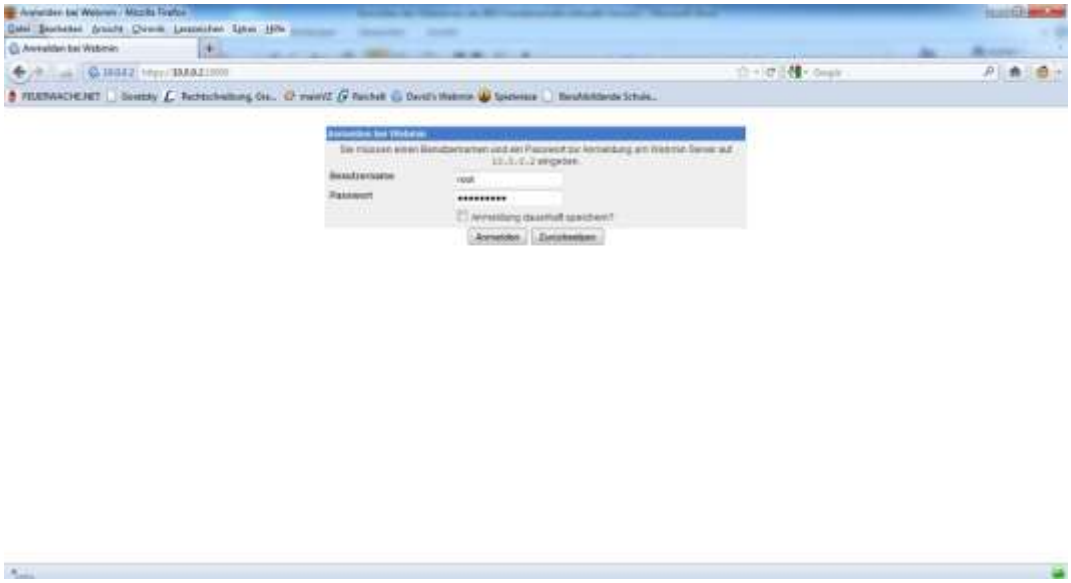


Abbildung 4- 2: Webmin Anmeldebildschirm

Nach der Eingabe des Benutzers root und des dazugehörigen Passworts gelangt man auf die Webmin Übersicht.

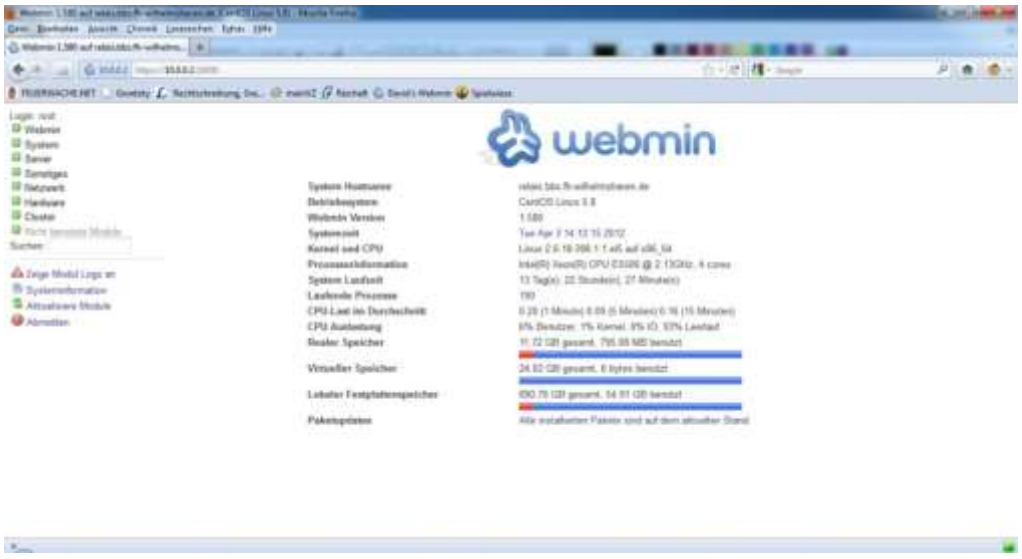


Abbildung 4- 3: Systeminformation

Mit Webmin haben wir die Netzwerkkonfigurationen, Sendmail, Apache, MySQL geändert und eingestellt.

4.3 Netzwerk

In den Netzwerkeinstellungen haben wir auf die Schnittstelle eth0 die IP-Adresse 10.60.107.101 zugewiesen, diese war unsere Verbindung in das Schulnetz, die IP wurde uns von Herrn Linnemann für den Webserver zugeteilt. Der Schnittstelle eth1 haben wir die IP-Adresse 10.0.0.2 zugewiesen, diese wird später die Verbindung aus dem Internet sein.

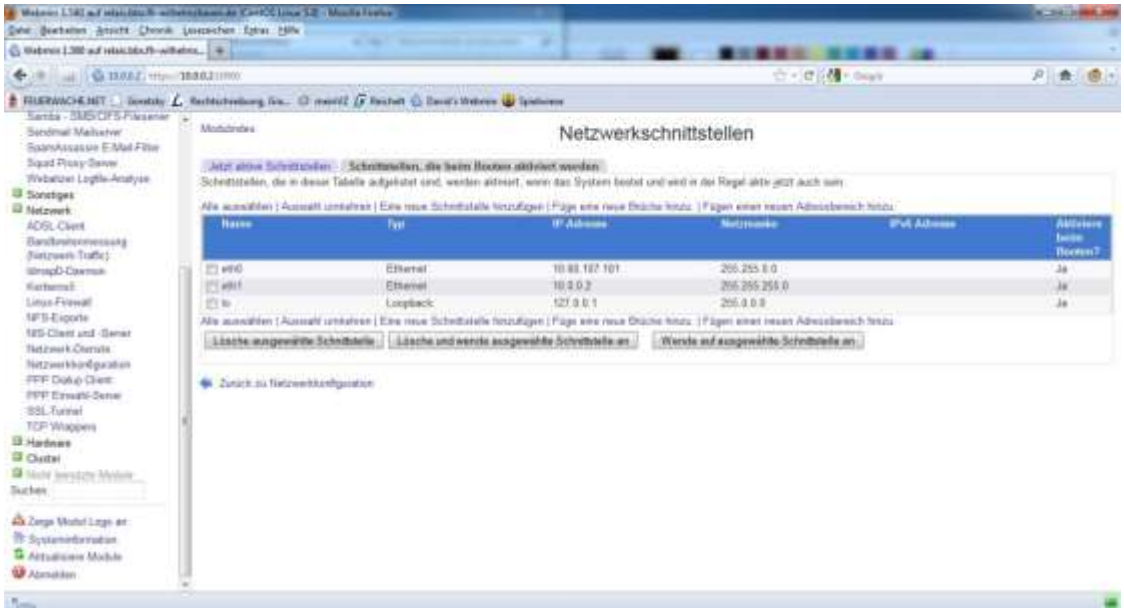


Abbildung 4- 4: Netzwerkkonfiguration - Netzwerkschnittstellen

Zum Testen haben wir unser eigenes Internet mit einem Laptop (IP:10.0.0.3) und einem Server (IP:10.0.0.1), auf dem der DNS Server läuft, aufgebaut, diesen DNS-Server haben wir auch in unsere DNS Konfiguration eingetragen.

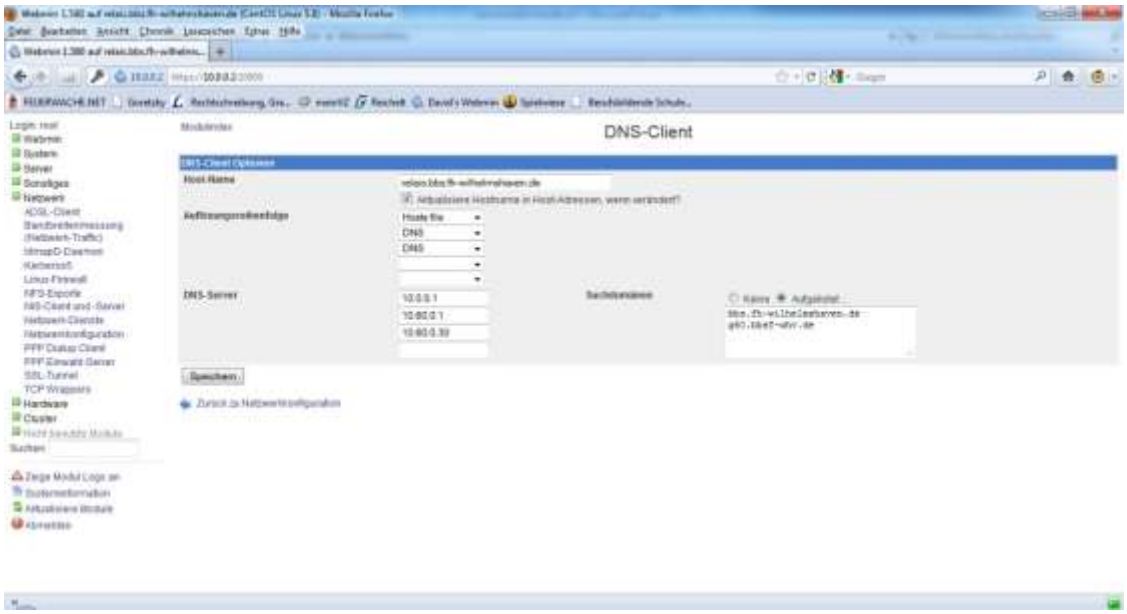


Abbildung 4- 5: Netzwerkkonfigurationen - DNS-Client

Nachdem die Hostadressen angepasst wurden, war die Konfiguration des Netzwerkes fertig.

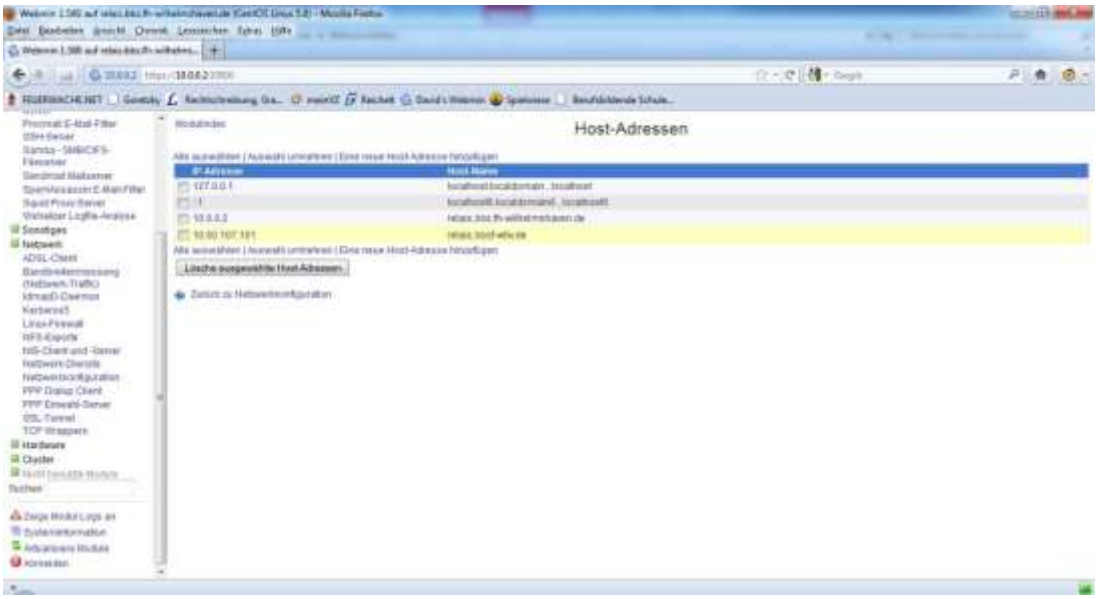


Abbildung 4- 6: Netzwerkkonfigurationen - Host-Adressen

4.4 NTP

Da der Webserver in der Demilitarisierten Zone der BBS Friedenstrasse steht, kann er den Super Server nicht erreichen und muss sich seine Systemzeit aus dem Internet holen. Dazu haben wir, nach Absprache mit Herrn Linnemann, in der ntp.conf noch den Zeitserver de.pool.ntp.org zusätzlich zu den CentOS Zeitservern eingetragen.

4.5 Sendmail

Sendmail als Mail Transfer Agent (MTA).

Abbildung 4- 7: Sendmail Mailserver - Konfigurationen

Der Webserver fungiert in der BBS als Email Relais für alle Mails an die Domänen:

bbsf-whv.de
bbs2.fh-wilhelmshaven.de
bbs.fh-wilhelmshaven.de

Diese Domänen haben wir als Weiterleitungsdomänen eingetragen.

Abbildung 4- 8: Sendmail Mailserver - Weiterleitungsdomänen

Um diese Emails an den vorhandenen Mailserver weiterleiten zu können, haben wir die Domänen noch in das Domänen-Routing eingetragen.

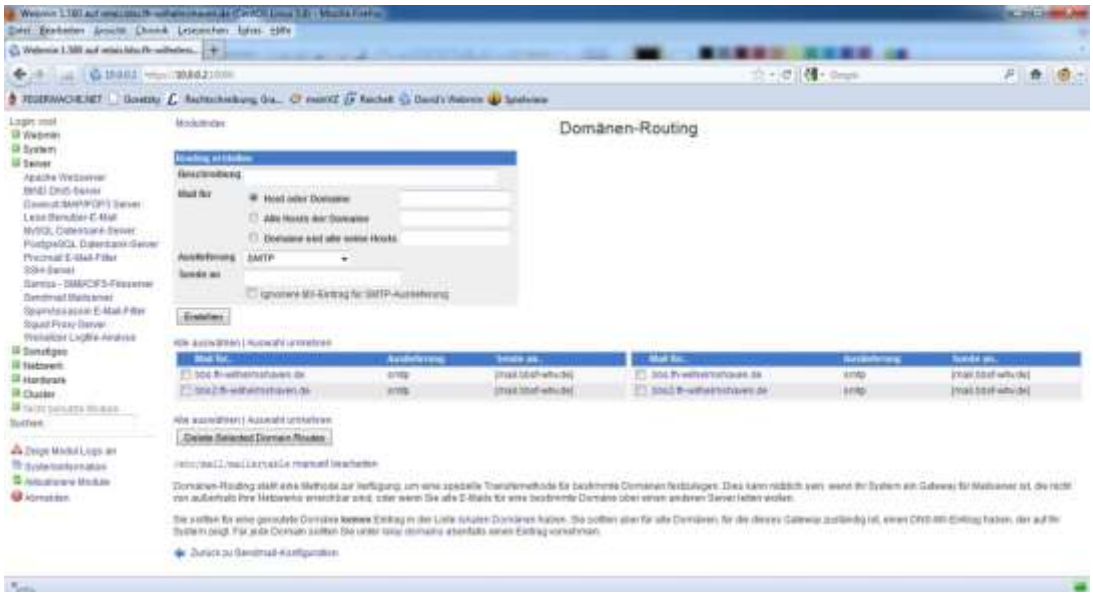


Abbildung 4- 9: Sendmail Mailserver - Domänen Routing

Damit der Webserver die Mails auch annimmt und über den smtp Port weiterleitet, haben wir die Einträge noch unter dem Menüpunkt Netzwerkports gemacht.

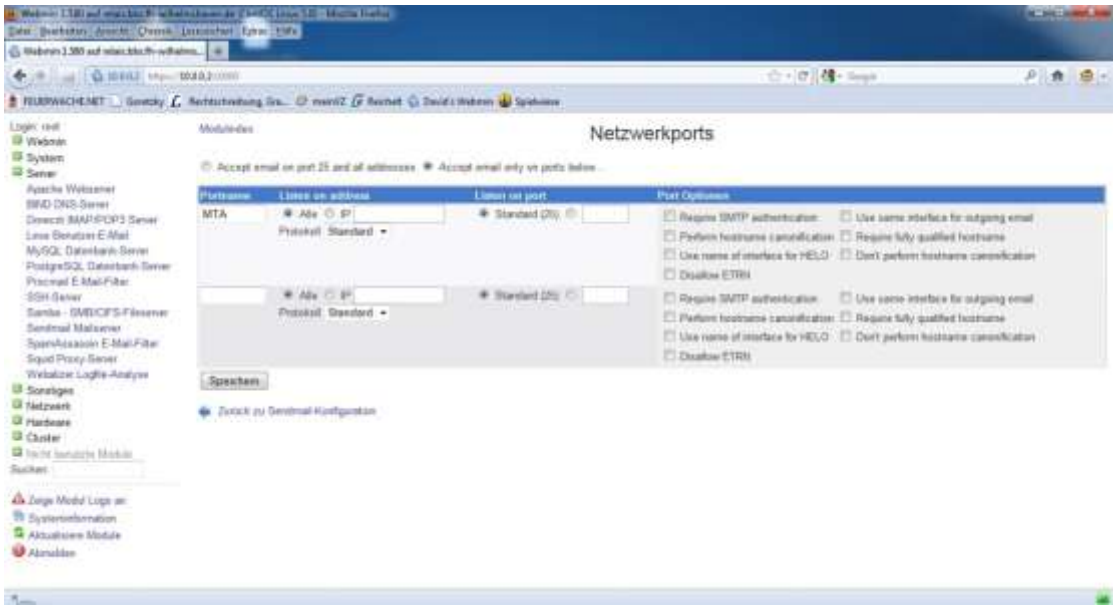


Abbildung 4- 10: Sendmail Mailserver - Netzwerkports

Damit die Systemmails auch versandt werden können, haben wir die Domänenmaskierung eingestellt.

Abbildung 4- 11: Sendmail Mailserver - Domänenmaskierung

Danach haben wir die Einstellungen der vertrauten Benutzer (nur eingetragene Benutzer können Mails versenden) und der lokalen Domänen gemacht.

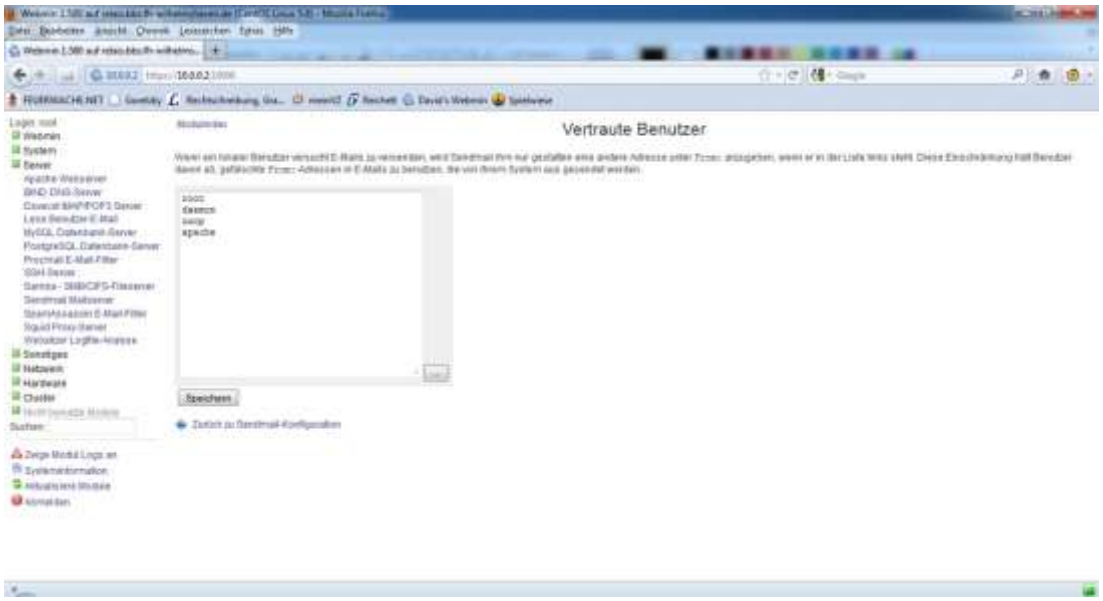


Abbildung 4- 12: Sendmail Mailserver - Vertraute Benutzer

Abbildung 4- 13: Sendmail Mailserver - Lokale Domänen

Zum Empfangen der System E-Mails haben wir auf einen zweiten Laptop Thunderbird installiert und eine Schüler Email Adresse eingerichtet, auf diese haben wir alle Mails, die später an den Administrator gehen müssen, umgeleitet.

4.6 Avira AntiVir MailGate

Die aktuelle Datei antivir-mailgate-prof.tgz haben wir uns von der Homepage http://www.avira.com heruntergeladen, mit dem Befehl
tar -xzvf antivir-mailgate-prof.tgz
entpackt und dann die Installation nach Anleitung mit dem Befehl ./install gestartet.
Während der Installation haben wir noch die Datei hbedv.key mit dem aktuellen Lizenzkey, die wir uns von Herrn Linnemann besorgt hatten, eingefügt.
Nach der Installation haben wir die Konfigurationsdateien mit den Dateien des Super-Servers verglichen und unsere Konfiguration an diese angepasst.

Konfigurationsdateien:

/etc/avira/avmailgate.conf	(Avira MailGate main config)
/etc/avira/avmailgate-scanner.conf	(Avira MailGate scanners config)
/etc/avira/avmailgate.acl	(Avira MailGate accesslist)
/etc/avira/avmailgate.ignore	(Avira MailGate ignore List)
/etc/avira/avmailgate.scan	(Avira MailGate Scan List)
/etc/avira/avmailgate.warn	(Avira MailGate Warn List)
/etc/avira/asmailgate.exept	(Avira MailGate Spamfilter Config)
/etc/avira/avupdate-mailgate.conf	(Avira AV Update Options)

Um das MailGate in Sendmail zu integrieren haben wir folgende Zeile in die sendmail.mc eingefügt.

INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,F=T,T=S:2m;R:2m;E:10m')

Da der Webserver den Hostnamen localhost nicht richtig auflösen konnte, haben wir den Eintrag localhost durch die IP-Adresse 127.0.0.1 ersetzt.

Damit die Binärdateien nicht vom System verändert werden können, musste der folgende Eintrag in der Datei /etc/prelink.conf gemacht werden.

-b /usr/lib/AntiVir/mailgate

Den geforderten SPAM-Schutz konnten wir nicht einrichten, da die Lizenz der Schule nicht für den SPAM-Schutz ausgelegt ist.

4.7 Apache Webserver

Durch die Übernahme der Typo3 Datenbanken des alten Webservers sind 2 Virtuelle Server in den Apache Webserver hinzugefügt worden. Diese sind für die korrekte Portweiterleitung und die Anzeige der BBS Webseite notwendig.

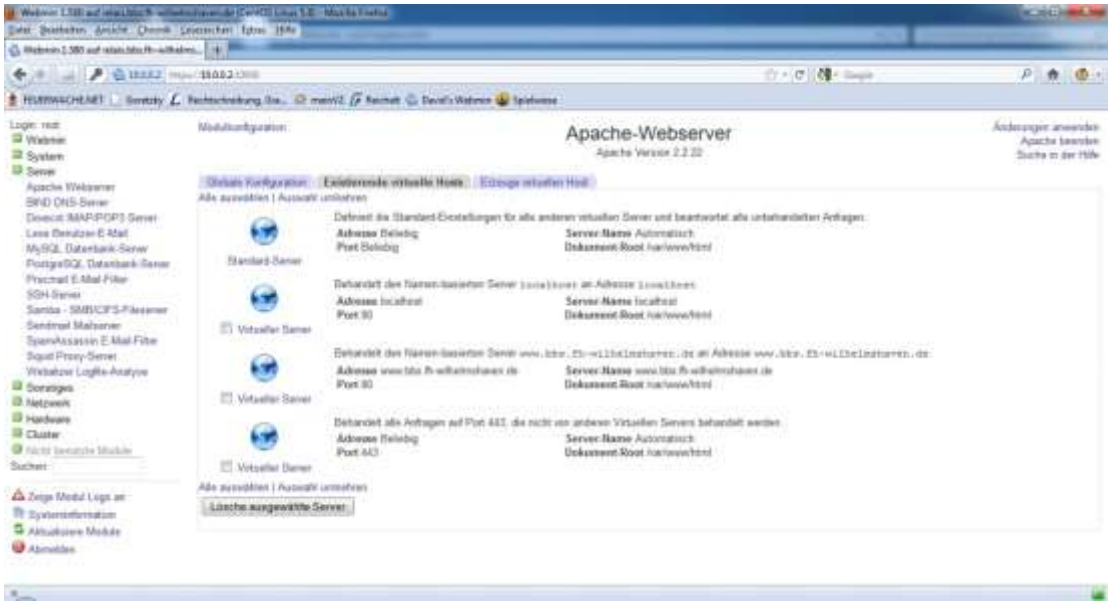


Abbildung 4- 14: Apache-Webserver

4.8 USV

Für den Datenaustausch zwischen der APC Smart-UPS 700 und dem Webserver haben wir folgende Einträge in der /etc/apcupsd/apcupsd.conf verändert.

UPSCABLE 940-1524C (Kabeltype variable einzutragen)
UPSTYPE apcsmart
DEVICE /dev/ttyS0

Die aktuelle Statusanzeige der UPS kann man sich unter https://localhost/apcupsd/upsstats.cgi anzeigen lassen.
In der Datei /etc/apcupsd/hosts.conf haben wir die IP-Adresse und den Namen des Super Servers und die des Webservers eingetragen. Dadurch kann man sich in dem APCUPSD UPS Network Monitor unter https://localhost/apcupsd/multimon.cgi den Status beider Rechner und der angeschlossen USV-Geräten anzeigen lassen.

4.9 Typo3

Nach der Übernahme der Typo3 Datenbanken haben wir die Ordnerstruktur, für die Übernahme der PragmaMX Seiten aus dem alten Techniker Portal, erweitert und vervollständigt. Nun konnten wir Dokumentationen und Bilder aus dem alten Portal heraus in die neue Ordnerstruktur kopieren. Danach haben wir für jedes Projekt der Jahre 1997 – 2008 eine neue Typo3 Seite erstellt, einen kleinen Beschreibungstext verfasst, die Autoren eingetragen, die Bilder eingefügt und die Dokumentationen verlinkt.

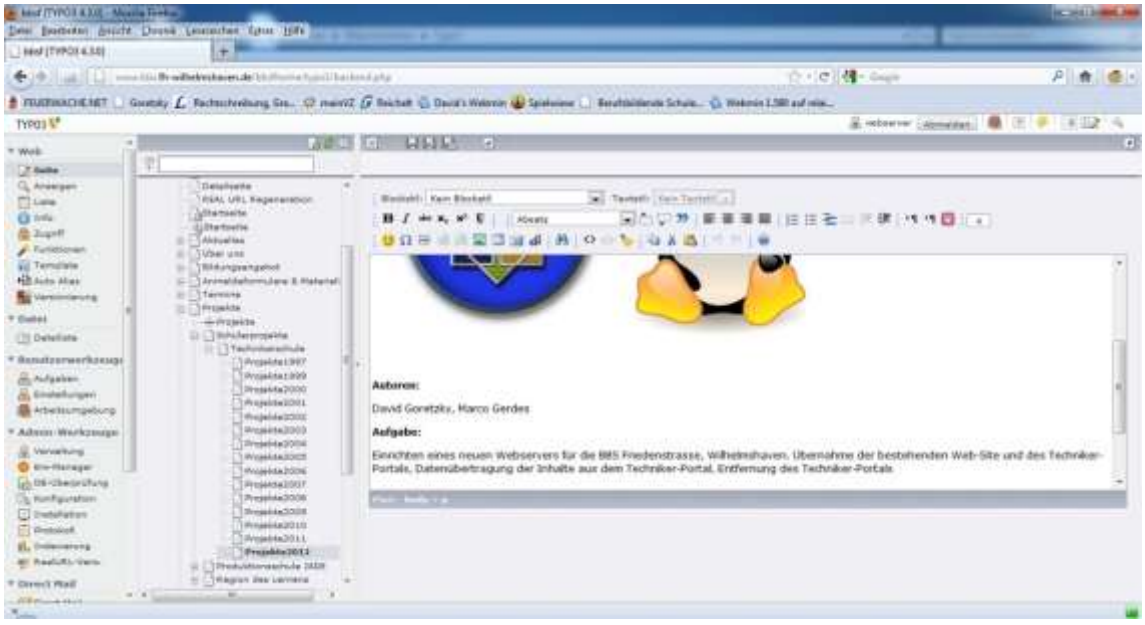


Abbildung 4- 15: Typo3 Oberfläche mit Rich-Text-Editor

4.10 Testrechner Konfiguration

Für unsere Testumgebung haben wir uns unser eigenes Internet mit eigenem DNS Server aufgebaut und eingerichtet. Im DNS Server haben wir die erste Master Zone für den Webserver mit dem Namen bbs.fh-wilhelmshaven.de eingerichtet. Für den Test-Rechner (Server) und den Laptop haben wir eine zweite Master Zone mit dem Namen testweb.de eingerichtet. Beide Masterzonen greifen auf die Reverse Zone 10.0.0 zu, die ebenfalls von uns eingerichtet wurde.

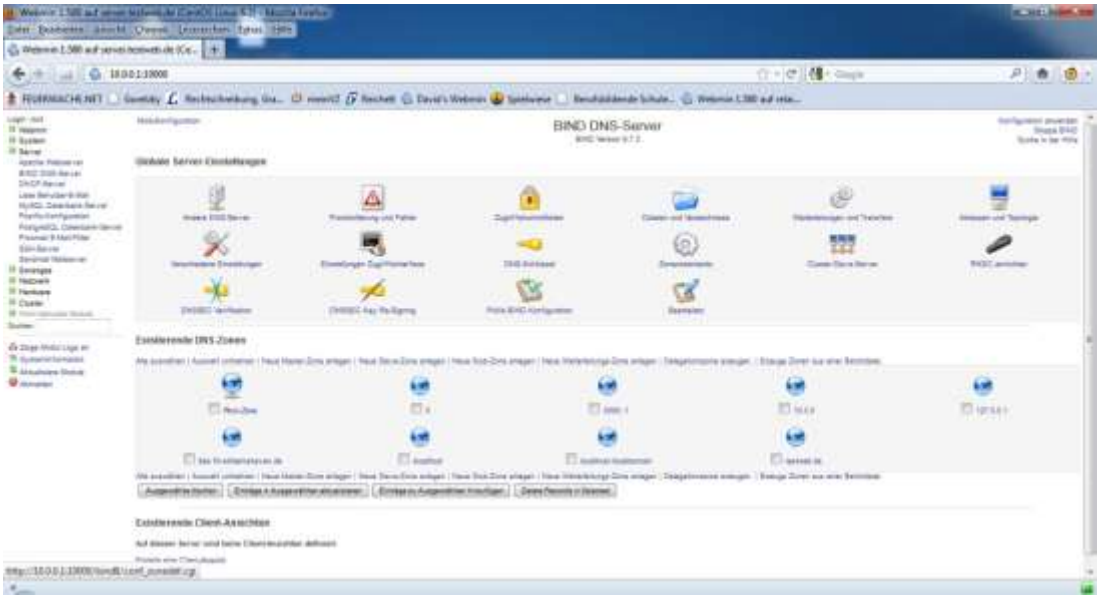


Abbildung 4- 16: Bind DNS-Server

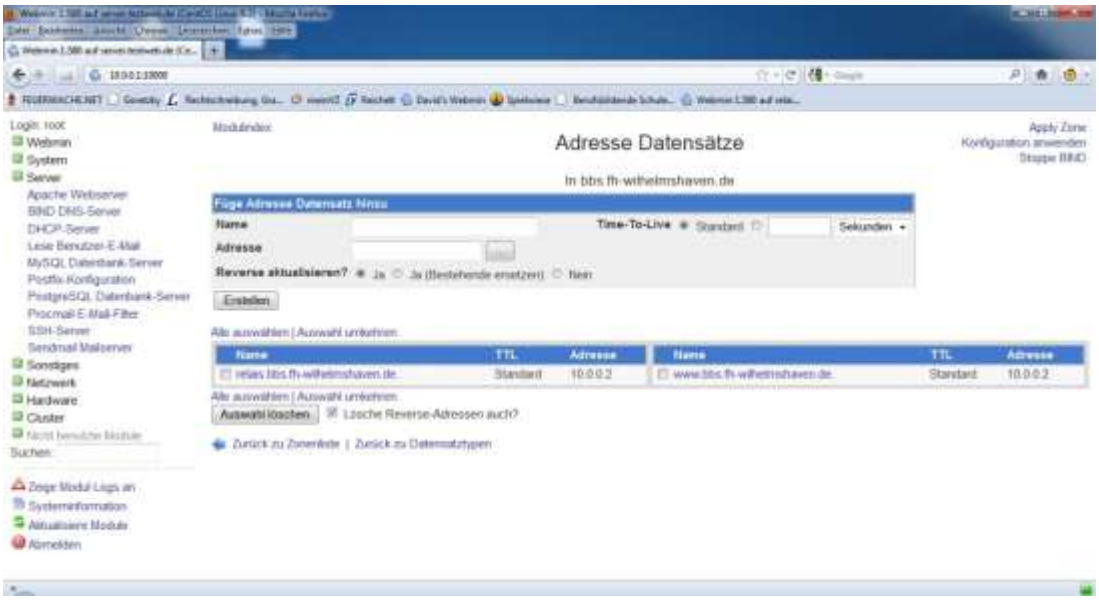


Abbildung 4- 17: Bind DNS-Server Masterzone bbs.fh-wilhelmshaven.de

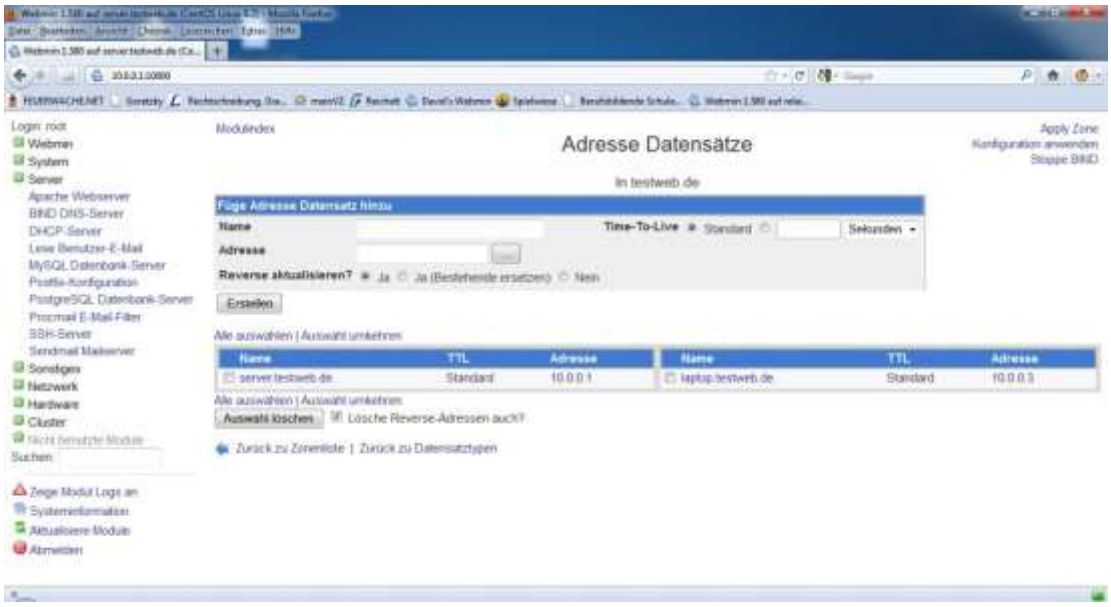


Abbildung 4- 18: Bind DNS-Server Masterzone testweb.de

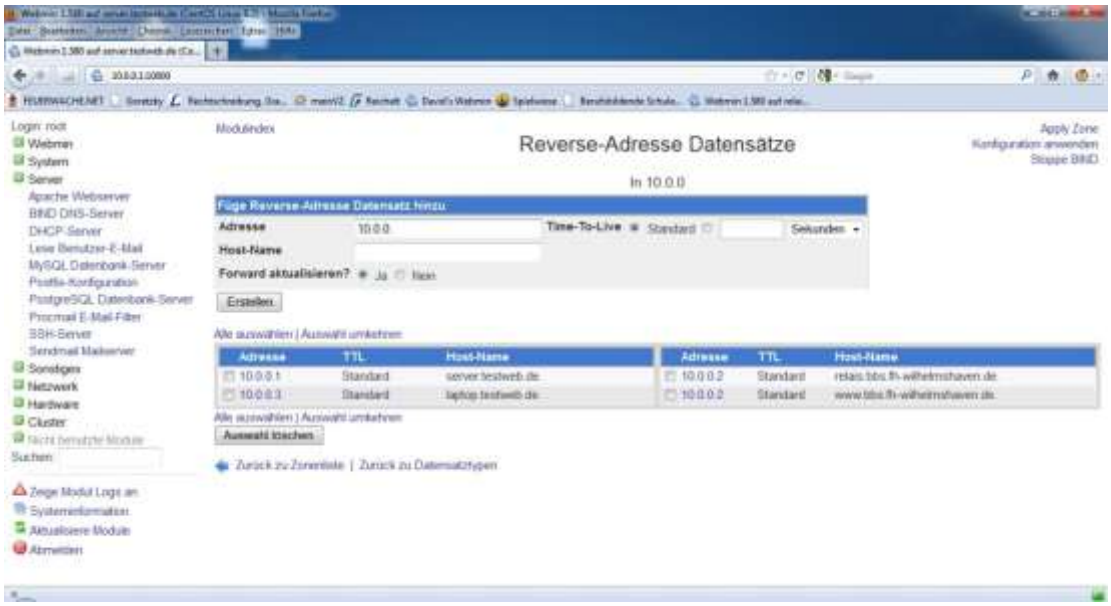


Abbildung 4- 19: Bind DNS-Server Reverse-Adresse Datensätze

5. Fazit

Nach erfolgreicher Beendigung des Projektes und der gewonnen distanzierten Betrachtungsweise gilt es zu sagen, dass dieses Projekt viele Herausforderungen barg. Durch zu voreiliges und nicht gut reflektiertes Handeln kam es zu dem Resultat, dass zahlreiche Programme mehrmals konfiguriert werden mussten und folglich wertvolle Zeit verloren ging.

Glücklicherweise standen uns Herr Appenzeller und Herr Linnemann tatkräftig zur Seite, denn manche Probleme wären ohne das Fachwissen der beiden viel weitläufiger geworden.
Dieses Projekt hat uns gezeigt, dass es wichtig ist, Ratschläge zu befolgen, genaue Planungen und präzise Abläufe zu erstellen und eine detaillierte Dokumentation zu führen.

Die Übergabe des voll funktionsfähigen Webservers an die BBS Friedenstraße erfüllt uns mit Stolz. Die gesamte Projektphase war eine Bereicherung für beide Beteiligten, der Lernzuwachs und das Umsetzen anfänglicher Visionen im stetigen Austausch mit dem Projektpartner waren hilfreich für das Vertiefen der von uns verlangten Kompetenzen.

Es bleibt noch zu sagen, dass ein gutes Zeit-Management das Allerwichtigste bei solchen Projekten ist. Herzlichen Dank an alle beteiligten Personen, die immer ein offenes Ohr für uns hatten.

6. Literaturverzeichnis / Internetquellen

6.1 Foren

http://ubuntuusers.de
http://serversupportforum.de/forum/webmin/1795-webmin-und-sendmail.html
12.04.2012

6.2 Elektronische Nachschlagewerke

http://de.wikipedia.org
http://www.linuxfibel.de
http://linuxwiki.de
http://de.linwiki.org
http://wiki.centos.org

6.3 Internetquellen, Installations-Informationen und Handbücher

http://www.avira.com
14.02.2012
http://avira.com/de/support-for-business-knowledgebase-detail/kbid/757
14.02.2012
http://www.avira.com/de/download-start/product/avira-antivir-mailgate
14.02.2012
http://www.avira.com/documents/products/pdf/de/man_avira_antivir-unix_mailgate_de.pdf
14.02.2012
http://www.avira.com/de/support-for-business-knowledgebase-detail/kbid/51
02.04.12
http://www.centos.org
07.02.2012
http://typo3.org
29.03.2012
http://pkgs.org
14.02.2012
http://pkgs.repoforge.org/rpmforge-release
14.02.2012
http://www.webmin.com
08.02.2012
http://www.techienote.com/2009/05/installing -php5-2-on-centos5-2.html
22.03.2012

7. Projekttagebuch

18.01.2012 Mittwoch

- Ist-Zustand ermittelt
- Hardware überprüft
- Mit CentOS 6.2 Live-Mode den Webserver gestartet
- Mac Adressen von eth0 und eth1 herausgesucht, damit das Betriebssystem Updates beziehen kann

24.01.2012 Dienstag

- Eingebautes CD Laufwerk gegen mitgeliefertes DVD Laufwerk getauscht
- CentOS 6.2 Installation
    - Probleme: CentOS 6.2 konnte aufgrund der werkseitigen Raid Konfiguration nicht zu installieren werden
    - Maßnahmen: Installation versucht über kubuntu, Ubuntu 11.10, Fedora 16. Fedora 16 wurde erfolgreich installiert und daraufhin haben wir versucht das bestehende Linux Betriebssystem mit CentOS 6.2 zu ersetzen. Dies war erfolgreich, dennoch brach der Webserver beim Bootvorgang ab.
    - Grund: Partitionierung der Festplatten wurde nicht übernommen

26.01.2012 Donnerstag

- Partitionieren der Festplatten, das Einrichten des, vom Projektleiter vorgegebenen, Software-Raids.
- Aufteilung sieht wie folgt aus:
    - **sda1, sdb1 = ext4** **md0 /boot**
    - **sda2, sdb2 = swap**
    - **sda3, sdb3 = ext4** **md1 /**
    - **sda4, sdb4 = erweiterte Partition**
    - **sda5, sdb5 = ext4** **md2 /opt**

01.02.2012 Mittwoch

- Installation von CentOS 6.2
    - erfolgreich abgeschlossen
    - Problem: Grub Installation erfolgte nur in den MBR der sda1 von md0

02.02.2012 Donnerstag

- Überprüfung der Installation CentOS 6.2:
    - Grub auf beiden Festplatten im md0 (sda1, sdb1) eingerichtet, damit der Bootvorgang von beiden Festplatten möglich ist
    - Bios Einstellungen überprüft und korrigiert (Festplattenmode IDE)
    - Einstellungen zum Bios im Internet recherchiert

- Hardwaretest durchgeführt

- IP Adresse von Herrn Linnemann erhalten für den Internetzugang. IP Adresse ist: 10.60.107.101 für die Schnittstelle eth0.
- yum update (Installieren der Updates)
- Synchronisierung der Festplatten

07.02.2012 Dienstag (08:00 bis 15:00 Uhr)

(Projektstart = Webserver im Dauerbetrieb, um Hardwaretauglichkeit für Dauerbetrieb zu testen)

- Nach der Update Installation fährt das Betriebssystem nicht mehr hoch.
  - F11 für Laufwerksauswahl = DVD Laufwerk ausgewählt
  - Entf = Bios
  - Tab = Hardware und Softwareboot in Konsolenebene anschauen
  - Strg + Alt + Entf = Systemneustart (Affengriff)
  - Strg + i = Raid-konfiguration, nur wenn im Bios Raid ausgewählt wurde
  - Rettungsmodus der Installations-DVD aufgerufen, um den Kernel wieder herzustellen, da auch ein Kernelupdate installiert wurde

  - Grub installiert in /dev/sda und in /dev/sdb
  - Betriebssystem startet wieder
  - Konfiguration des Betriebssystems begonnen
  - Befehle:
    - cat /proc/mdstat
    - /etc/selinux/conig (SELINUX = disabled)
    - chkconfig (kdump = off)
    - system-config-network, joe und viele weitere Pakete nicht installiert

Downgrade auf CentOS 5.5

- Installation von CentOS 5.5
- Partitionieren der Festplatten, das Einrichten des, vom Projektleiter vorgegebenen, Software-Raids.
- Aufteilung sieht wie folgt aus:
  - **sda1, sdb1 = ext3** **md0 /boot**
  - **sda2, sdb2 = swap**
  - **sda3, sdb3 = ext3** **md1 /**
  - **sda4, sdb4 = erweiterte Partition**
  - **sda5, sdb5 = ext3** **md2 /opt**
- Server, Server GUI und KDE Desktop gewählt
- bei der Installation SELINUX deaktiviert
- Installation erfolgreich abgeschlossen
- Synchronisierung der Festplatten
- Einrichten des Proxys in der Datei /etc/yum.conf mit der Konfiguration proxy=http://10.1.0.1:8080
  - keepcache =1 (Update-Informationen zwischenspeichern)
  - debuglevel = 2 (Standard), Auswahl von 1 bis 10
- joe installiert = yum install joe
- yumex installiert = yum install yumex

- Netzwerkmanager installiert = yum install system-config-network (beinhaltet: system-config-network und system-config-network-tui)
- Sendmail installiert = yum install sendmail (sendmail, sendmail –cf)

08.02.2012 Mittwoch (08:00 bis 15:00 Uhr)

- MBR auf beide Festplatten im md0 (sda1, sdb1) eingerichtet, damit der Bootvorgang von beiden Festplatten möglich ist
    - Befehle, um Grub in beide Festplatten zu schreiben:
        - Konsole als root
        - Befehl:
        - grub
        - root (hd0,0)
        - setup(hd0)
        - root(hd1,0)
        - setup(hd1)
- Partitionen wieder einhängen
    - Befehle:
        - mdadm /dev/md0 --add /dev/sdb1
        - mdadm /dev/md1 --add /dev/sdb3
        - mdadm /dev/md2 --add /dev/sdb
        - sync startet dann automatisch
        - cat /proc/mdstat (Sync-Status überprüfen)
- Hardwaretest durchgeführt und abgeschlossen
- Testrechner installiert mit kubuntu 11.10, Bios konfiguriert und MAC Adresse von eth0 rausgesucht
- APC Smart-UPS 700 (http://pkgs.org/centos-5-rhel-5/rpmforge-x86_64/apcupsd-3.14.8-1.el5.rf.x86_64.rpm)
    - Download apcupsd-3.14.8-1.el5.x86_64.rpm
    - yum localinstall --nogpgcheck apcupsd-3.14.8-1.el5.x86_64.rpm
    - joe /etc/apcupsd/apcupsd.conf
        - UPSCABLE 940-1524C (Kabeltype variable einzutragen)
        - UPSTYPE apcsmart
        - DEVICE /dev/ttyS0
    - service apcupsd start (Dienst starten)
    - service apcupsd status (Status der SmartUPS anzeigen)
    - Download apcupsd-cgi-3.14.8-1.el5.x86_64.rpm
    - yum localinstall --nogpgcheck apcupsd-cgi-3.14.8-1.el5.x86_64.rpm
    - service httpd start (Dienst starten)
    - erreichbar im Browser unter: https://localhost/apcupsd/
- Download rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
    - yum localinstall --nogpgcheck rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
- Download webmin-1.580-1.noarch.rpm
    - yum localinstall --nogpgcheck webmin-1.580-1.noarch.rpm
    - erreichbar im Browser unter: (https://localhost:1000/)
        - Benutzername: root
        - Passwort: webserver

09.02.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Updates installiert (800MB)

10.02.2012 Freitag (08:00 bis 09:30 Uhr)

- Update Kontrolle (CentOS wurde von 5.5 auf 5.7 gesetzt)
- Festplatte sdb ausgehängt, um den Hardwaretest der Festplatte sda durchzuführen
- Partition wieder einhängen
    - Befehle:
        - mdadm /dev/md0 --add /dev/sda1
        - mdadm /dev/md1 --add /dev/sda3
        - mdadm /dev/md2 --add /dev/sda5
        - sync startet dann automatisch
        - cat /proc/mdstat (Sync-Status überprüfen)
- Hardwaretest durchgeführt und abgeschlossen

14.02.2012 Dienstag (08:00 bis 15:00 Uhr)

- ein Update wurde nicht installiert (apcupsd-cgi)
- rpm -qi apcupsd (Versionskontrolle)
- yum erase apcupsd-cgi (deinstallieren)
- yum update (apcupsd wurde geupdatet)
- in der neuen apcupsd ist die apcupsd-cgi enthalten, Browseraufruf der APC-SmartUPS jetzt über https://localhost/apcupsd/upsstats.cgi (Normaler Status) und https://localhost/apcupsd/multimon.cgi (Alle im Netzwerk vorhandenen UPS-Geräte)
- In der /etc/apcupsd/hosts.conf die IP und den Namen des Super Servers eingetragen, um die Funktion von multimon zu testen
- Kontrolle der Pakete mysql, php, httpd auf neuen und alten Webserver
    - mysql: 5.0.77-4 (neu) 5.0.45-6 (alt)
    - php: 5.1.6-27 (neu) 5.2.6-2 (alt)
    - httpd: 2.2.3-53 (neu) 2.2.8-1 (alt)
- Avira Mailgate Downloaden von http://avira.com/de/support-for-business-knowledgebase-detail/kbid/757
- aus dem Download-Ordner avira_redhat.repo in den Ordner /etc/yum.repos.d verschoben
- Yumex aufgerufen und unter Available avira-mailgate gedownloadet (49MB)
- Avira-Mailgate laut Anleitung installiert (siehe nachfolgende Seiten)
- von Herrn Linnemann hbedv.key bekommen um Avira Mailgate zu aktivieren. Diesen in den Downloadordner verschoben und bei der Installation dorthin verwiesen
    - AntiVir Core Components (Engine, Savapi, Avupdate)
    - Avira Internet Updater
    - Avira MailGate
    - AntiVir SMC plugin

- Configurationfiles:
  - /etc/avira/avmailgate.conf (Avira MailGate main config)
  - /etc/avira/avmailgate-scanner.conf (Avira MailGate scanners config)
  - /etc/avira/avmailgate.acl (Avira MailGate accesslist)
  - /etc/avira/avmailgate.ignore (Avira MailGate ignore List)
  - /etc/avira/avmailgate.scan (Avira MailGate Scan List)
  - /etc/avira/avmailgate.warn (Avira MailGate Warn List)
  - /etc/avira/asmailgate.exept (Avira MailGate Spamfilter Config)
  - /etc/avira/avupdate-mailgate.conf (Avira AV Update Options)
- Integration von Avira AntiVir MailGate (Milter Modus) in Sendmail (Seite 14 Handbuch)
- Konfiguration Avira AntiVir MailGate (ab Seite 30 Handbuch)
- httpd (Apache) unter System, Dienste gesetzt damit beim Systemstart httpd bootet
- konfigurieren der mdadm.conf
- konfigurieren der apcupsd.conf
- konfigurieren der httpd.conf

15.02.2012 Mittwoch (08:00 bis 15:00 Uhr)

- Maskierung der localen Mail Adresse root@localhost.localdomain, um Mails weiterzuleiten an ein bestehendes E-Mail Konto auf den BBS-Mailserver
- aktuelle E-Mail Adresse David Goretzky in die /etc/avira/avupdate-mailgate.conf (email-to = s103058@bbs.fh-wilhelmshaven.de) eingefügt und E-Mail Adresse von Herrn Linnemann auskommentiert
- in der /etc/avira/avupdate-mailgate.conf notify-when = 1 gesetzt, damit er erstmals Mails versendet, wenn Updates erfolgreich waren, wenn Updates nicht erfolgreich waren und wenn keine Updates zur Verfügung stehen
- in der /etc/aliases ebenfalls die E-Mail von Herrn Linnemann auskommentiert und die E-Mail Adresse von David Goretzky eingetragen in den Abschnitt Person who shut get root´s mail
- über Installation von Typo3 informiert

16.02.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Konfiguration von Thunderbird auf dem Testrechner um Mails vom Webserver abzurufen, die seit dem 15.02.2012 versendet wurden
- E-Mails kommen an (Sendmail und Maskierung funktionieren)
- Maskierung und Mailversand funktionieren (Avira, local und UPS)

21.02.2012 Dienstag (08:00 bis 15:00 Uhr)

- Informationen über DNS gesammelt und Testrechner vorbereitet für die DNS Servernutzung
- Material von Herrn Linnemann geholt (Switch, Crossover Kabel, Patch Kabel), um ein eigenes Netz aufzubauen für die Webserver Testumgebung
- Netz aufgebaut und Schnittstellen konfiguriert
- Testrechner auf aktuellen Stand gebracht (yum update)

22.02.2012 Mittwoch (08:00 bis 15:00 Uhr)

- Testrechner als DNS Server eingerichtet
  - Schritt 1:
    - In Webmin auf Netzwerke, Netzwerkkonfiguration, Netzwerkschnittstelle und dort die Netzwerkschnittstelle eth0 mit der IP 10.0.0.1/24 zugewiesen. MTU auf Standard gesetzt und Schnittstelle eth0 bei Booten aktiviert.
  - Schritt 2:
    - In Webmin auf dem Server, BIND DNS Server installiert und dort eine neue Master-Zone (Forward) eingerichtet mit dem Domainnamen: testweb.de, Master-Server: server.testweb.de, E-Mail: root@server.testweb.de. Daraufhin noch die Reverse-Zone dazu mit der Konfiguration Netzwerk: 10.0.0, Masterserver: server.testweb.de und der E-Mail: root@server.testweb.de
  - Schritt 3:
    - Adressen in der Master-Zone unter Adressen eingetragen.
      - Testrechner (Name: server, Adresse: 10.0.0.1)
      - Webserver (Name: webserver, Adresse: 10.0.0.2)
      - Laptop (Name: laptop, Adresse: 10.0.0.3)
  - Schritt 4:
    - In der Konsole folgende Befehle eingegeben, damit BIND DNS Server startet ohne Fehlermeldung.
      - tail -f /var/log/messages (Fehlermeldungsnachricht lesen)
      - chmod 644 /etc/named.conf (damit alle die Datei /etc/named.conf lesen können, weil keine chroot Umgebung vorhanden ist)
      - joe /etc/resolv.conf (hier eintragen: domain: testweb.de und nameserver: 10.0.0.1)
      - nslookup laptop, nslookup server, nslookup webserver, um zu sehen, ob die Vorwärtsauflösung funktioniert
      - nslookup 10.0.0.1, nslookup 10.0.0.2, nslookup 10.0.0.3, um zu sehen, ob die Rückwärtsauflösung funktioniert
- sendmail auf Testrechner installiert
- Laptop zum Mailversand vorbereitet und ins eigene Netz eingebunden

23.02.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Internet Verbindung wieder hergestellt
- Sendmail Konfiguration angefangen

28.02.2012 Dienstag (08:00 bis 15:00 Uhr)

- Sendmail konfiguriert
- Neuen Benutzer auf Testrechner angelegt (Benutzername: server; PW: server)

29.02.2012 Mittwoch (08:00 bis 15:00 Uhr)

- Sendmail konfiguriert
- Thunderbird konfiguriert
- Privates Netz erstellt (testweb.de) und Webserver so eingerichtet, dass Emails an s103058@bbs.fh-wilhelmshaven verschickt werden (Email Relais Test).

01.03.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Thunderbird konfiguriert
- Sendmail konfiguriert

06.03.2012 Dienstag (08:00 bis 15:00 Uhr)

- Master Zone (bbs.fh-wilhelmshaven.de) für den mail Versand im eigenen Internet
- Netzwerkkonfiguration - DNS Client Konfiguration angepasst
- Testvirus verschickt, der vom SUPER Server abgefangen wurde
- Avmailgate.conf
  - Postmaster einkommentiert
  - EnableLegacyQuarantine YES einkommentiert

07.03.2012 Mittwoch (08:00 bis 15:00 Uhr)

- Avmailgate.conf
  - Postmaster auskommentiert
  - EnableLegacyQuarantine YES auskommentiert
- 1.Laptop als DNS Server konfiguriert auf dem Basissystem Ubuntu 11.10
- 2.Laptop zum Verschicken interner Mails im eigenen privaten Netz vorbereitet

08.03.2012 Donnerstag (11:30 bis 13:05 Uhr)

- von Herrn Linnemann die avmailgate.conf vom Super Server und Webserver geholt
- diese Dateien verglichen
- jetziger Webserver läuft ohne Virenschutz

13.03.2012 Dienstag (08:00 bis 15:00 Uhr)

- avmailgate.conf vom neuen Webserver und dem Super-Server abgeglichen
- Einstellungen überarbeitet und angepasst

14.03.2012 Mittwoch (08:00 bis 15:00 Uhr)

- DNS Konfigurationen dokumentiert und angepasst
  - Netzwerkkonfigurationen:
    - DNS - Client

- Host-Name: g0107s101
- Haken für Systemweite Übernahme nicht gesetzt

  - Auflösungsreihenfolge:
    - DNS
    - DNS
  - DNS Server:
    - 10.60.0.1
    - 10.60.0.30
  - Suchdomänen:
    - Aufgelistet:
      - g60.bbsf-whv.de

- Sendmail Konfigurationen dokumentiert und angepasst
  - Netzwerk-Ports:
    - Name: MTA
    - Accept email only on ports below = Port 25
    - listen on address = Alle
    - keine Haken gesetzt
  - Mail-Aliases:
    - root = s103058@bbs.fh-wilhelmshaven.de (Goretzky)
    - Auskommentiert = Linnemann@bbs.fh-wilhelmshaven.de
  - Lokale Domänen:
    - localhost
    - localhost.localdomain
  - Domänenmaskierung:
    - Maskiere als Domäne g0107s101
    - Domänen die Maskiert werden sollen:
      - localhost
      - localhost.localdomain
  - Vertraute Benutzer:
    - root
    - daemon
    - uucp
    - apache
  - Domänen-Routing:
    - bbs.fh-wilhelmshaven.de
    - bbs2.fh-wilhelmshaven.de
    - .bbs.fh-wilhelmshaven.de
    - .bbs2.fh-wilhelmshaven.de
    - Ausliefern über: SMTP
    - Sende an: mail.bbsf-whv.de
  - Spamkontrolle:
    - Domain:
      - localhost.localdomain
      - localhost
      - 127.0.0.1
      - Passend auf = Verbindungsinformationen
      - Aktion = Akzeptieren

  - Weiterleitungsdomänen:
    - bbsf-whv.de
    - bbs2.fh-wilhelmshaven.de
    - bbs.fh-wilhelmshaven.de
- Die lokalen Domänen und die Domänenmaskierung wurden in der Sendmail m4 Konfiguration geändert
- in der /etc/hosts stehen folgende Einträge:
  - 127.0.0.1 localhost.localdomain localhost
  - ::1 localhost6.localdomain6 localhost6
- in der /etc/HOSTNAME steht folgender Eintrag:
  - g0107s101
- einen kleinen Überblick einer m4 Konfiguration für eine T-Online Weiterleitung erhält man auf der Webseite http://serversupportforum.de/forum/webmin/1795-webmin-und-sendmail.html

15.03.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Alle Konfigurationsdateien fürs Mailgate vom Super-Server geholt
  - Asmailgate.except
  - Avmailgate.acl
  - Avmailgate.conf
  - Avmailgate.groups
  - Avmailgate.ignore
  - Avmailgate-odbc.ini
  - Avmailgate.scan
  - Avmailgate-scanner.conf
  - Avmailgate.warn
  - Avupdater-mailgate.conf

20.03.2012 Dienstag (08:00 bis 15:00 Uhr)

- AvMailgate neu installiert und an die geholten Konfigurationsdateien vom Super-Server angepasst
- Test des Sendmail Virenschutzes
- negativ verlaufen

21.03.2012 Mittwoch (08:00 bis 15:00 Uhr)

- weiterhin AV-Mailgate bearbeitet und Informationen im Internet gesucht
- Dokumentation bearbeitet

22.03.2012 Donnerstag (09:30 bis 13:30 Uhr)

- Laut der Konfigurationsanleitung auf der Seite http://www.techienote.com/2009/05/installing-php5-2-on-centos5-2.html installiert. Folgende Befehle als root ausgeführt

```
touch /etc/yum.repos.d/utterramblings.repo
echo '[utterramblings]' >> /etc/yum.repos.d/utterramblings.repo
echo "name=Jason's Utter Ramblings Repo" >> /etc/yum.repos.d/utterramblings.repo
echo 'baseurl=http://www.jasonlitka.com/media/EL$releasever/$basearch/' >>
/etc/yum.repos.d/utterramblings.repo
echo 'enabled=1' >> /etc/yum.repos.d/utterramblings.repo
echo 'gpgcheck=1' >> /etc/yum.repos.d/utterramblings.repo
echo 'gpgkey=http://www.jasonlitka.com/media/RPM-GPG-KEY-jlitka' >>
/etc/yum.repos.d/utterramblings.repo
```

- yum list updates
- rpm -q mysql,pcre Versionen geprüft
- yum update
- yum update php
- rpm -q php
- pcre-6.6-6.EL5_6.1.i386 deinstalliert
- yum install pcre (erfolglos)
    - yum update pcre
- yum erase mysql-5.0.95-1.EL5_7.1.i386 deinstalliert
- yum list update
- yum update
- rpm -q mysql
- rpm -q ImageMagick
- rpm -qa |grep kdebase
- Typo3 SQL Datendanken und Webseite auf Webserver kopiert und angepasst.
    - SQL Datenbanken in SQL Webserver eingefügt
    - Webseite in Ordner /var/www/html eingefügt und entpackt
- chmod a-x httpd.conf
- ps ax |grep http
- über Yumex php-mysql installiert
- service httpd restart
- service mysqld restart
- NetworkManager unter Dienste beim Bootvorgang abgeschaltet
- Hostname geändert auf relais.bbs.fh-wilhelmshaven.de
- Localen DNS Server in der MasterZone bbs.fh-wilhelmshaven auf neuen Hostnamen relais angepasst und in diese Zone ebenfalls www eingetragen damit die Webseite erreichbar und auflösbar im lokalen Netz ist.
- mit Herrn Gerdes (Typo3 Betreuer) Einweisung von TYPO3 durchgeführt
    - Webseite wird auf aktiven Webserver geändert und diese wird mit neuen Webserver synchronisiert
    - Benutzername und Passwort für Typo3 Konfigurationen erhalten

28.03.2012 Mittwoch (09:00 bis 15:00 Uhr)

- Typo3 Ordner Struktur zur Übernahme der PragmaMX Dateien erstellt
- Dokumentation bearbeitet

29.03.2012 Donnerstag (08:30 bis 15:00 Uhr)

- Typo3 Ordner Struktur weiter bearbeitet und abgeschlossen
- Dokumentation bearbeitet

02.04.2012 Montag (09:00 bis 15:00 Uhr)

- alle Avira Ordner gelöscht und alle Programme deinstalliert
- AvMailgate neu installiert um zu sehen, ob das unkonfigurierte Programm ebenfalls nicht startet
- AVUpdate.conf an die selbige vom Super-Server angeglichen (Proxyusername = super, PW = antivir, Email = root@localhost)
- Testrechner als DNS - Server eingerichtet
- E-Mail Abruf über Laptop realisiert (Thunderbird)
- Domänenmaskierung von relais.bbs.fh-wilhelmshaven.de in m4 Konfiguration eingetragen, Maskiert wird auf webserver2012
- AvMailgate konnte aktiviert werden, als MTA Port von Sendmail auf willkürlichen Port geändert wurde. Der Standart-Port ist 25 und dieser wird von AvMailgate belegt.
  http://www.avira.com/de/support-for-business-knowledgebase-detail/kbid/51
    - ggf. für Sendmail anderen Port wählen

03.04.2012 Dienstag (09:00 bis 15:00 Uhr)

- AvMailgate in Sendmail integriert laut nachfolgender Anleitung
    - Avira Milter is included in Avira MailGate

  since version 2.1.0-0.
  Please consult the MILTER_MIGRATION documentation to see how you
  can migrate from Avira Milter to Avira MailGate.
  NOTE:
  Your sendmail installation must support MILTER.
  To find out if sendmail supports MILTER, do the following:
  sendmail -d0.10 < /dev/null | grep MILTER
  Installation instructions
  ==========
  1. Install Avira MailGate by using the install script
  ---
  cd ..
  ./install
  2. Configure Avira MailGate

  Set "ListenAddress" and "ForwardTo" in /etc/avira/avmailgate.conf:

ListenAddress inet:3333@localhost
ForwardTo /usr/lib/sendmail -oem -oi
3. Insert the following line in your sendmail.mc:

INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,F=T,T=S:2m;R:2m;E:10m')
- 'avmilter' is the name of the filter
- S= defines how the filter can be reached
{unix|local}:/path/to/file
inet:port@{hostname|ip-address}
(Must be the same as in your avmailgate.conf 'ListenAddress')
- F= defines what sendmail will do if the filter can not be reached:
R means reject connection if filter is unavailable
T means temporary fail connection if filter is unavailable
- T= sets the following timeouts:
C: Timeout for connecting to a filter. If set to 0,
the system's connect() timeout will be used. Default: 5m
S: Timeout for sending information from the MTA to a filter. Default: 10s
R: Timeout for reading reply from the filter. Default: 10s
E: Overall timeout between sending end-of-message to filter
and waiting for the final acknowledgment. Default: 5m
If you encounter errors in the log, like "Milter (avmilter): timeout before data read",
try to raise the timeout values.
If you use other filters, define the order in which they
will be called:
E.g.:
define(`confINPUT_MAIL_FILTERS', `avmilter,filter2,filter1,filter3')
4. Build sendmail and start services

- Build sendmail.cf and restart sendmail.
- Start Avira MailGate:
/usr/lib/AntiVir/mailgate/avmailgate start
5. Send mail and check log

Send a test mail to yourself and check the log file (/var/log/mail*).
If you find an entry "X-AntiVirus: checked by Avira MailGate"
in the log, the mail was scanned.
You can also have a look at the header of the mail you received
to check for the X-AntiVirus header.

04.04.2012 Mittwoch (09:00 bis 15:00 Uhr)

- Sendmail bearbeitet
- DNS Server bearbeitet
- Dokumentation bearbeitet

12.04.2012 Donnerstag (11:30 bis 13:05 Uhr)

- bei Herrn Linnemann und Herrn Appenzeller über die Portvergabe bei Sendmail und AvMailgate informiert
- in den Dateien avmailgate.conf, sendmail.cf und sendmail.mc alles, was localhost hieß, in 127.0.0.1 umbenannt
- avmailgate.acl Carriage Return fehlte
- in der /etc/host.conf die Zeilen order hosts, bind und multi on hinzugefügt
- in der /etc/hosts 10.60.107.101 mit relais.bbsf-whv.de und 10.0.0.2 mit relais.bbs.fh-wilhelmshaven.de eingetragen und entsprechend die graphische Netzwerkeinrichtung und Webmin Netzwerkkonfiguration angepasst
- Hostnamen in der /etc/HOSTNAME geändert in relais.bbs.fh-wilhelmshaven.de und auch in der graphischen Netzwerkeinrichtung und in Webmin Netzwerkkonfigurationen angepasst
- DNS Server in der graphischen Netzwerkeinrichtung und Suchdomänen angepasst sowie in Webmin auch
- die /etc/resolv.conf kontrolliert
- Portkontrolle von AvMailgate und Sendmail mit dem Befehl natstat -tulpen
- durch die vorher beschriebenen Punkte laufen AvMailgate und Sendmail jetzt zusammen
- AvMailgate läuft über den Port 3333 und Sendmail über den Port 25

17.04.2012 Dienstag (08:00 bis 14:55 Uhr)

- AvMailgate Viren Test durchgeführt. Dieser war erfolgreich, siehe folgenden Mail:

* * * * * * * * * * * * * * * Avira MailGate ALERT * * * * * * * * * * * * * * *

Avira MailGate has detected the following in a mail sent through your server:
(1x) Eicar-Test-Signature (type: virus)
The mail was not delivered.
It has been quarantined with the following queue id:
10968-kKiqdt
Mail-Info:
--8<--
Message-Id: <1334646171.6497@laptop.testweb.de>
Sender: fedora@laptop.testweb.de
To: webserver@relais.bbs.fh-wilhelmshaven.de
Date: Tue, 17 Apr 2012 09:02:51 +0200 (CEST)
Subject: hihi
Mail-From: fedora@laptop.testweb.de
Rcpt: webserver@relais.bbs.fh-wilhelmshaven.de
Queue-Id: 10968-kKiqdt
Status: The mail was not delivered!
--8<--
Mail-Header:
--8<--
Received: from laptop.testweb.de (localhost [127.0.0.1])
by laptop.testweb.de (8.14.5/8.14.5) with ESMTP id q3H72pru006598
for <webserver@relais.bbs.fh-wilhelmshaven.de>; Tue, 17 Apr 2012 09:02:51 +0200
Received: (from root@localhost)
by laptop.testweb.de (8.14.5/8.14.5/Submit) id q3H72pwb006597
for webserver@relais.bbs.fh-wilhelmshaven.de; Tue, 17 Apr 2012 09:02:51 +0200
From: fedora@laptop.testweb.de
Subject: hihi

To: webserver@relais.bbs.fh-wilhelmshaven.de

Message-Id: <1334646171.6497@laptop.testweb.de>
X-Originating-IP: 127.0.0.1
X-Mailer: Webmin 1.580
Date: Tue, 17 Apr 2012 09:02:51 +0200 (CEST)
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="bound1334646171"
--8<--

18.04.2012 Mittwoch (08:00 bis 14:55 Uhr)

- Dokumentation bearbeitet

19.04.2012 Donnerstag (11:30 bis 13:05 Uhr)

- PDF Dateien und Bilder verschoben auf laufenden Webserver von PragmaMX in Typo3
- alte CDs durchsucht nach Dokumentationen
- Dokumentation bearbeitet

24.04.2012 Dienstag (08:00 bis 14:55 Uhr)

- Datenbanken in MySQL eingebunden
- Backup der Datenbanken funktioniert nicht. Fehlermeldung im Internet recherchiert
- Dokumentation bearbeitet

25.04.2012 Mittwoch (08:00 bis 14:55 Uhr)

- Fehlermeldung beim Backup der Datenbanken nach der Anleitung unter http://dev.mysql.com/doc/refman/5.1/en/upgrading.html und http://dev.mysql.com/doc/refman/5.1/en/mysql-upgrade.html mit dem Befehl mysql_upgrade –u webserver –password=webserver behoben
- Um diesen Befehl ausführen zu können, haben wir noch den User webserver mit allen Rechten erstellt
- Typo3 Seiten bearbeitet
- alte Datenbanken entfernt
- Dokumentation bearbeitet

26.04.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Datenbanken übernommen und neu eingebunden
- veraltete Datenbanken entfernt
- /var/www/html strukturiert und geordnet

02.05.2012 Mittwoch (08:00 bis 14:55 Uhr)

- Dokumentation bearbeitet

03.05.2012 Donnerstag (11:30 bis 13:05 Uhr)

- Dokumentation bearbeitet

08.05.2012 Dienstag (08:00 bis 14:55 Uhr) Projektende

- Dokumentation bearbeitet

8. Konfigurationsdateien

8.1 /etc/resolv.conf

/etc/resolv.conf Row 4 Col 1 11:42 Ctrl-K H for help
nameserver 10.0.0.1
nameserver 10.60.0.1
nameserver 10.60.0.30
domain g60.bbsf-whv.de
search bbs.fh-wilhelmshaven.de g60.bbsf-whv.de

8.2 /etc/host.conf

/etc/host.conf Row 3 Col 1 11:43 Ctrl-K H for help
order hosts,bind
multi on

8.3 /etc/hosts

/etc/hosts Row 3 Col 1 11:43 Ctrl-K H for help

Do not remove the following line, or various programs

that require network functionality will fail.

127.0.0.1 localhost.localdomain localhost

::1 localhost6.localdomain6 localhost6

10.0.0.2 relais.bbs.fh-wilhelmshaven.de

10.60.107.101 relais.bbsf-whv.de

8.4 /etc/HOSTNAME

/etc/HOSTNAME Row 1 Col 1 11:44 Ctrl-K H for help

relais.bbs.fh-wilhelmshaven.de

8.5 /etc/mdadm.conf

mdadm.conf written out by anaconda

DEVICE partitions

MAILADDR root

ARRAY /dev/md1 level=raid1 num-devices=2 uuid=863c527a:b8497ac8:e1eec745:87b294a1

ARRAY /dev/md2 level=raid1 num-devices=2 uuid=dbf1aa12:d1dcd3b9:017417c3:00af12d9

ARRAY /dev/md0 level=raid1 num-devices=2 uuid=38a8e413:7e1d4109:f9eb644d:1f7c4d46

8.6 /etc/apcupsd/apcupsd.conf

apcupsd.conf v1.1

#

for apcupsd release 3.14.8 (16 January 2010) - redhat

#

"apcupsd" POSIX config file

#

========= General configuration parameters ============

#

UPSNAME xxx

Use this to give your UPS a name in log files and such. This

is particulary useful if you have multiple UPSes. This does not

set the EEPROM. It should be 8 characters or less.

#UPSNAME

UPSCABLE <cable>

Defines the type of cable connecting the UPS to your computer.

#

Possible generic choices for <cable> are:

```
#     simple, smart, ether, usb
#
#   Or a specific cable model number may be used:
#     940-0119A, 940-0127A, 940-0128A, 940-0020B,
#     940-0020C, 940-0023A, 940-0024B, 940-0024C,
#     940-1524C, 940-0024G, 940-0095A, 940-0095B,
#     940-0095C, M-04-02-2000
#
UPSCABLE 940-1524C
# To get apcupsd to work, in addition to defining the cable
# above, you must also define a UPSTYPE, which corresponds to
# the type of UPS you have (see the Description for more details).
# You must also specify a DEVICE, sometimes referred to as a port.
# For USB UPSes, please leave the DEVICE directive blank. For
# other UPS types, you must specify an appropriate port or address.
#
# UPSTYPE   DEVICE          Description
# apcsmart  /dev/tty**      Newer serial character device, appropriate for
#                           SmartUPS models using a serial cable (not USB).
#
# usb       <BLANK>         Most new UPSes are USB. A blank DEVICE
#                           setting enables autodetection, which is
#                           the best choice for most installations.
#

# net       hostname:port   Network link to a master apcupsd through apcupsd's
#                           Network Information Server. This is used if the
#                           UPS powering your computer is connected to a
```

```
#                   different computer for monitoring.
#
# snmp      hostname:port:vendor:community
#                   SNMP network link to an SNMP-enabled UPS device.
#                   Hostname is the ip address or hostname of the UPS
#                   on the network. Vendor can be can be "APC" or
#                   "APC_NOTRAP". "APC_NOTRAP" will disable SNMP trap
#                   catching; you usually want "APC". Port is usually
#                   161. Community is usually "private".
#
# netsnmp   hostname:port:vendor:community
#                   OBSOLETE
#                   Same as SNMP above but requires use of the
#                   net-snmp library. Unless you have a specific need
#                   for this old driver, you should use 'snmp' instead.
#
# dumb      /dev/tty**      Old serial character device for use with
#                   simple-signaling UPSes.
#
# pcnet     ipaddr:username:passphrase
#                   PowerChute Network Shutdown protocol which can be
#                   used as an alternative to SNMP with the AP9617
#                   family of smart slot cards.ipaddr is the IP
#                   address of the UPS mgmtcard. username and
#                   passphrase are the credentials for which the card
#                   has been configured.
#
```

UPSTYPE apcsmart

DEVICE /dev/ttyS0

POLLTIME <int>

Interval (in seconds) at which apcupsd polls the UPS for status. This

setting applies both to directly-attached UPSes (UPSTYPE apcsmart, usb,

dumb) and networked UPSes (UPSTYPE net, snmp). Lowering this setting

will improve apcupsd's responsiveness to certain events at the cost of

higher CPU utilization. The default of 60 is appropriate for most

situations.

#POLLTIME 60

LOCKFILE <path to lockfile>

Path for device lock file. Not used on Win32.

LOCKFILE /var/lock

SCRIPTDIR <path to script directory>

Directory in which apccontrol and event scripts are located.

SCRIPTDIR /etc/apcupsd

PWRFAILDIR <path to powerfail directory>

Directory in which to write the powerfail flag file. This file

is created when apcupsd initiates a system shutdown and is

checked in the OS halt scripts to determine if a killpower

(turning off UPS output power) is required.

PWRFAILDIR /etc/apcupsd

NOLOGINDIR <path to nologin directory>

Directory in which to write the nologin file. The existence

of this flag file tells the OS to disallow new logins.

NOLOGINDIR /etc

#

======== Configuration parameters used during power failures ==========

```
#
# The ONBATTERYDELAY is the time in seconds from when a power failure
#   is detected until we react to it with an onbattery event.
#
#   This means that, apccontrol will be called with the powerout argument
#   immediately when a power failure is detected.  However, the
#   onbattery argument is passed to apccontrol only after the
#   ONBATTERYDELAY time.  If you don't want to be annoyed by short
#   powerfailures, make sure that apccontrol powerout does nothing
#   i.e. comment out the wall.
ONBATTERYDELAY 6
#
# Note: BATTERYLEVEL, MINUTES, and TIMEOUT work in conjunction, so
# the first that occurs will cause the initation of a shutdown.
#
# If during a power failure, the remaining battery percentage
# (as reported by the UPS) is below or equal to BATTERYLEVEL,
# apcupsd will initiate a system shutdown.
BATTERYLEVEL 5
# If during a power failure, the remaining runtime in minutes
# (as calculated internally by the UPS) is below or equal to MINUTES,
# apcupsd, will initiate a system shutdown.
MINUTES 3
# If during a power failure, the UPS has run on batteries for TIMEOUT
# many seconds or longer, apcupsd will initiate a system shutdown.
# A value of 0 disables this timer.
#
#  Note, if you have a Smart UPS, you will most likely want to disable
```

```
#    this timer by setting it to zero. That way, you UPS will continue
#    on batteries until either the % charge remaing drops to or below BATTERYLEVEL,
#    or the remaining battery runtime drops to or below MINUTES.  Of course,
#    if you are testing, setting this to 60 causes a quick system shutdown
#    if you pull the power plug.
#  If you have an older dumb UPS, you will want to set this to less than
#    the time you know you can run on batteries.
TIMEOUT 0
#  Time in seconds between annoying users to signoff prior to
#  system shutdown. 0 disables.
ANNOY 300
# Initial delay after power failure before warning users to get
# off the system.
ANNOYDELAY 60
# The condition which determines when users are prevented from
# logging in during a power failure.
# NOLOGON <string> [ disable | timeout | percent | minutes | always ]
NOLOGON disable
# If KILLDELAY is non-zero, apcupsd will continue running after a
# shutdown has been requested, and after the specified time in
# seconds attempt to kill the power. This is for use on systems
# where apcupsd cannot regain control after a shutdown.
# KILLDELAY <seconds>  0 disables
KILLDELAY 0
#
# ==== Configuration statements for Network Information Server ====
#
# NETSERVER [ on | off ] on enables, off disables the network
```

information server. If netstatus is on, a network information

server process will be started for serving the STATUS and

EVENT data over the network (used by CGI programs).

NETSERVER on

NISIP <dotted notation ip address>

IP address on which NIS server will listen for incoming connections.

This is useful if your server is multi-homed (has more than one

network interface and IP address). Default value is 0.0.0.0 which

means any incoming request will be serviced. Alternatively, you can

configure this setting to any specific IP address of your server and

NIS will listen for connections only on that interface. Use the

loopback address (127.0.0.1) to accept connections only from the

local machine.

NISIP 0.0.0.0

NISPORT <port> default is 3551 as registered with the IANA

port to use for sending STATUS and EVENTS data over the network.

It is not used unless NETSERVER is on. If you change this port,

you will need to change the corresponding value in the cgi directory

and rebuild the cgi programs.

NISPORT 3551

If you want the last few EVENTS to be available over the network

by the network information server, you must define an EVENTSFILE.

EVENTSFILE /var/log/apcupsd.events

EVENTSFILEMAX <kilobytes>

By default, the size of the EVENTSFILE will be not be allowed to exceed

10 kilobytes. When the file grows beyond this limit, older EVENTS will

be removed from the beginning of the file (first in first out). The

parameter EVENTSFILEMAX can be set to a different kilobyte value, or set

```
#  to zero to allow the EVENTSFILE to grow without limit.
EVENTSFILEMAX 10
#
# ========== Configuration statements used if sharing =============
#           a UPS with more than one machine
#
# Remaining items are for ShareUPS (APC expansion card) ONLY
#
# UPSCLASS [ standalone | shareslave | sharemaster ]
#   Normally standalone unless you share an UPS using an APC ShareUPS
#   card.
UPSCLASS standalone
# UPSMODE [ disable | share ]
#   Normally disable unless you share an UPS using an APC ShareUPS card.
UPSMODE disable
#
# ===== Configuration statements to control apcupsd system logging ========
#
# Time interval in seconds between writing the STATUS file; 0 disables
STATTIME 0
# Location of STATUS file (written to only if STATTIME is non-zero)
STATFILE /var/log/apcupsd.status
# LOGSTATS [ on | off ] on enables, off disables
# Note! This generates a lot of output, so if
#       you turn this on, be sure that the
#       file defined in syslog.conf for LOG_NOTICE is a named pipe.
#  You probably do not want this on.
LOGSTATS off
```

Time interval in seconds between writing the DATA records to

the log file. 0 disables.

DATATIME 0

FACILITY defines the logging facility (class) for logging to syslog.

If not specified, it defaults to "daemon". This is useful

if you want to separate the data logged by apcupsd from other

programs.

#FACILITY DAEMON

#

========== Configuration statements used in updating the UPS EPROM =========

#

#

These statements are used only by apctest when choosing "Set EEPROM with conf

file values" from the EEPROM menu. THESE STATEMENTS HAVE NO EFFECT ON APCUPSD.

#

UPS name, max 8 characters

#UPSNAME UPS_IDEN

Battery date - 8 characters

#BATTDATE mm/dd/yy

Sensitivity to line voltage quality (H cause faster transfer to batteries)

SENSITIVITY H M L (default = H)

#SENSITIVITY H

UPS delay after power return (seconds)

WAKEUP 000 060 180 300 (default = 0)

#WAKEUP 60

UPS Grace period after request to power off (seconds)

SLEEP 020 180 300 600 (default = 20)

#SLEEP 180

Low line voltage causing transfer to batteries

The permitted values depend on your model as defined by last letter

of FIRMWARE or APCMODEL. Some representative values are:

D 106 103 100 097

M 177 172 168 182

A 092 090 088 086

I 208 204 200 196 (default = 0 => not valid)

#LOTRANSFER 208

High line voltage causing transfer to batteries

The permitted values depend on your model as defined by last letter

of FIRMWARE or APCMODEL. Some representative values are:

D 127 130 133 136

M 229 234 239 224

A 108 110 112 114

I 253 257 261 265 (default = 0 => not valid)

#HITRANSFER 253

Battery charge needed to restore power

RETURNCHARGE 00 15 50 90 (default = 15)

#RETURNCHARGE 15

Alarm delay

0 = zero delay after pwr fail, T = power fail + 30 sec, L = low battery, N = never

BEEPSTATE 0 T L N (default = 0)

#BEEPSTATE T

Low battery warning delay in minutes

LOWBATT 02 05 07 10 (default = 02)

#LOWBATT 2

UPS Output voltage when running on batteries

```
# The permitted values depend on your model as defined by last letter
#  of FIRMWARE or APCMODEL. Some representative values are:
#    D 115
#    M 208
#    A 100
#    I 230 240 220 225     (default = 0 => not valid)
#OUTPUTVOLTS 230
# Self test interval in hours 336=2 weeks, 168=1 week, ON=at power on
# SELFTEST 336 168 ON OFF  (default = 336)
#SELFTEST 336
```

8.7 /etc/avira/avmailgate.conf

```
##############################################################################
##                    avmailgate.conf                      ##
##############################################################################
# This file lists all the available parameters. Lines beginning with '#'
# are comments and are ignored. If a parameter is not specified, the
# default value shown here is used. Note that not all option have a
# default value however.
#
# For each option, the data type is given as well.
#
# The following data types are currently in use:
#
# string
#   a sequence of one or more characters. If you want the value to start
#   or end with whitespace, you need to put the value in "quotation marks".
```

```
#
# number:
#   a decimal number.
#
# non-negative number:
#   a non-negative decimal number (0 or greater).
#
# boolean:
#   a boolean value ie either YES or NO.
#
# size:
#   a decimal number optionally followed by the suffix KB (kilobytes),
#   MB (megabytes) or GB (gigabytes). If no suffix is given,
#   the value is interpreted as bytes.
#
# timespan:
#   a decimal number optionally followed by the suffix s (seconds),
#   m (minutes), h (hours) or d (days). If no suffix is given,
#   the value is interpreted as seconds.
#
# ------------------------------------------------------------------------
# User [string]
# MailGate will switch to the user given here.
#
# IMPORTANT:
# When changing this option, you also have to change the option
# "User" in /etc/avira/avmailgate-scanner.conf.
# Otherwise the scanner backend cannot be reached anymore and
```

scan requests are no more possible.

You also need to adjust the permissions for the spool directory

(option SpoolDir) and for /usr/lib/AntiVir/mailgate/gui.

#

Default:

User uucp

Group [string]

MailGate will switch to the group given here.

See User.

#

Default:

Group antivir

Postmaster [string]

Who will get errors and alert messages.

#

Default:

Postmaster postmaster

MyHostName [string]

The FQDN of the local host.

The default value, if not set in configuration file, is that

obtained by gethostname(2), or if this fails, "localhost".

#

Example:

MyHostName localhost

```
# SpoolDir [string]
# The spooldir must be owned by User:Group (as specified above)
# and must be accessible by only this user (mode = 0700).
# Both programs will refuse to run if something is wrong.
#
# Default:
# SpoolDir /var/spool/avmailgate
# ------------------------------------------------------------------------
# EnableLegacyQuarantine [boolean]
# Set this option to 'NO' if you want to use the new quarantine feature
# of MailGate.
#
# Note: Please read the section "Quarantine management" in
# /usr/lib/AntiVir/mailgate/antivir_mailgate_en.txt before changing this option.
#
# Note: EnableLegacyQuarantine is not available in milter mode.
#
# Default:
# EnableLegacyQuarantine YES
# ------------------------------------------------------------------------
# AntiVirDir [string]
# The antivir 'library' directory, where the VDF, the key,
# and some other files are stored.
#
# Note: This must be set to /usr/lib/AntiVir/mailgate if anti-spam
#       is being used.
#
```

```
# Default:
# AntiVirDir /usr/lib/AntiVir/mailgate
# ----------------------------------------------------------------------
# TemporaryDir [string]
# Where the temporary files are stored (for example when changing the
# content of a mail).
# It needs enough space to hold uncompressed attachments
# for each forwarder, and some more.
# Default: "/var/tmp" or else "/tmp".
#
# IMPORTANT:
#
# You may want to change the option "ScanTemp" in MailGate's scanner
# specific configuration file (default /etc/avira/avmailgate-scanner.conf)
# to set a proper location for decompressing mails (you can use the same
# value for both parameters).
#
# If TemporaryDir is not set and the environment variable TMPDIR is set,
# the directory specified in TMPDIR will be used.
#
# Example:
# TemporaryDir /var/tmp
# ----------------------------------------------------------------------
# MatchMailAddressForLocal [string]
# You can set this option to RECIPIENT, SENDER or BOTH to allow matching of
# the domain name of the recipient and/or sender mail address, to check if it's
# to be considered local.
```

```
#
# If MatchMailAddressForLocal is RECIPIENT, and the recipient address matches
# the domain given in "local:", mail will be accepted.
#
# If MatchMailAddressForLocal is SENDER, and the sender address matches the
# domain given in "local:", mail will be accepted.
#
# If MatchMailAddressForLocal is BOTH, and the recipient or the sender addresses
# matches the domain given in "local:" mail will be accepted.
#
# Default:
# MatchMailAddressForLocal RECIPIENT
# ----------------------------------------------------------------------
# SMTPBanner [string]
# SMTP greeting message.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
SMTPBanner "Avira MailGate"
# ----------------------------------------------------------------------
# PidDir [string]
# Where the pid files are stored.
# Default: "/var/tmp" or else "/tmp".
#
# Example:
# PidDir /var/tmp
```

```
# ---------------------------------------------------------------------
# SyslogFacility [string]
# Specify the facility for the syslog.
#
# Example:
# SyslogFacility local0
#
# Default:
# SyslogFacility mail
# ---------------------------------------------------------------------
# LogFile [string]
# Specify a full path with a filename to which Avira MailGate
# will write its log messages. Avira MailGate still logs to syslog
# even if this option is set.
#
# To disable logging to a custom logfile, set this option to NO.
#
# Example:
# LogFile /var/log/avmailgate.log
#
# Default:
# LogFile NO
# ---------------------------------------------------------------------
# DebugLevel [non-negative number]
# The option DebugLevel specifies how much debug output is written
# to the syslog and, if enabled, to the log file (option "LogFile").
#
# Possible values are 0-5. 0 means no debug messages will be shown.
```

```
# 5 means all debug message will be shown.
#
# Default:
# DebugLevel 0
# ---------------------------------------------------------------------
# ListenAddress [string]
# Select the network interface the SMTP daemon will listen on.
# The default listen address of 0.0.0.0 means all interfaces.
# Note however that the default value will only be accepted if IPv4 is enabled
# (config option InetProtocols). If you disable IPv4 support, you will have
# to specify a valid IPv6 address here.
# Note that milter mode only works with IPv4 currently.
#
# IF YOU ARE UNSURE JUST LEAVE IT AS IS!
#
# To start Avira MailGate in milter mode, use the following:
#
# ListenAddress inet:port@{hostname|ip-address}
# E.g: ListenAddress inet:3333@localhost
#
# OR
#
# ListenAddress {unix|local}:/path/to/file
# E.g: ListenAddress unix:/path/to/file
#
# Default:
# ListenAddress "0.0.0.0 port 25"
ListenAddress inet:3333@127.0.0.1
```

```
# ---------------------------------------------------------------------
# MaxIncomingConnections [non-negative number]
# Limit the number of simultaneous connections from remote sites.
# A limit of 0 disables this feature.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# MaxIncomingConnections 0
# ---------------------------------------------------------------------
# SMTPTimeout [non-negative number]
# Number of seconds until a timeout occurs in SMTP conversation.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# SMTPTimeout 300
# ---------------------------------------------------------------------
# MaxMessageSize [non-negative number]
# Larger mails will be rejected.
# A limit of 0 means "no limit" (in bytes).
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# MaxMessageSize 0
# ---------------------------------------------------------------------
# MinFreeBlocks [non-negative number]
```

Refuse incoming connections if less free blocks are available

on the filesystem containing the spool directory.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

MinFreeBlocks 100

--

MaxRecipientsPerMessage [non-negative number]

So many recipients can be accepted at once.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

MaxRecipientsPerMessage 100

--

RefuseEmptyMailFrom [boolean]

Refuse 'MAIL FROM:<>'.

Actually, RFC2821, RFC821 and RFC2505 explicitly note that 'MAIL FROM: <>'

MUST be accepted. It is strongly recommended not to change the

default setting.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

RefuseEmptyMailFrom NO

```
# ---------------------------------------------------------------------
# AllowSourceRouting [boolean]
# If AllowSourceRouting is NO, if source routing is present in the
# given recipient address path, it's removed.
#
# If AllowSourceRouting is YES, then source routing is honored, and
# the message is forwarded to the first host specified in the route.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# AllowSourceRouting NO
# ---------------------------------------------------------------------
# InEnvelopeAddressesBangIs [string]
# If InEnvelopeAddressesBangIs is REFUSED, the presence of an unquoted
# "!" in the recipient envelope address implies that the message will be
# refused.
#
# If InEnvelopeAddressesBangIs is IGNORED, any unquoted "!" will be
# processed as any other non-special character of the address.
#
# If InEnvelopeAddressesBangIs is INTERPRETED, then the address is
# rewritten in RFC821 standard form. An address such as:
#
# hostA!hostB!hostC!user
#
# is rewritten as:
#
```

```
# @hostA,@hostB:user@hostC
#
# Then, if source routing is allowed, the message is transmitted to
# hostA, otherwise it's directly sent to hostC.
#
# Thus, this rewriting allows us to discover the recipient host, in the
# case where all the UUCP gateways on the route would have interpreted
# the address the same way as us. (If that were not the case, then this
# parameter should be set to IGNORED).
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# InEnvelopeAddressesBangIs REFUSED
# ----------------------------------------------------------------------
# InEnvelopeAddressesPercentIs [string]
# If InEnvelopeAddressesPercentIs is REFUSED, the presence of an
# unquoted "%" in the recipient envelope address implies that the message
# will be refused.
#
# If InEnvelopeAddressesPercentIs is IGNORED, any unquoted "%" will be
# processed as any other non-special character of the address.
#
# If InEnvelopeAddressesPercentIs is INTERPRETED, then the address is
# rewritten in RFC821 standard form. An address such as:
#
# user%hostC%hostB@hostA
#
```

is rewritten as:

#

@hostA,@hostB:user@hostC

#

Then, if source routing is allowed, the message is transmitted to

hostA, otherwise it's directly sent to hostC.

#

Thus, this rewriting allows us to discover the recipient host, in the

case where all the gateways on the route would have interpreted the

address the same way as us. (If that were not the case, then this

parameters should be set to IGNORED).

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

InEnvelopeAddressesPercentIs REFUSED

AcceptLooseDomainName [boolean]

If AcceptLooseDomainName is NO and the name of the domain selected

for delivery (depending on source routing) does not strictly conform

the domain name syntax, it's refused.

#

If AcceptLooseDomainName is YES, no check is done on the domain

name, apart of interpreting the domain name syntax for numerical IP

addresses.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

AcceptLooseDomainName NO

AddressFilter [boolean]

If AddressFilter is YES, the recipient address and/or the sender address of

an email will be matched against a table of addresses.

Two tables will be matched in a specified order (see option "FilterTableOrder").

Please have a look at /usr/lib/AntiVir/mailgate/antivir_mailgate_en.txt for more

details.

#

Default:

AddressFilter NO

FilterTableOrder [string]

If AddressFilter is set to yes, one can specify which table has to be matched

for a sender and/or recipient address first.

Options are: scan,ignore | ignore,scan

#

Default:

FilterTableOrder scan,ignore

SMTPGreetingTimeout [non-negative number]

Timeout, in seconds, to receive the greeting message from the remote host.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPGreetingTimeout 300

SMTPHeloTimeout [non-negative number]

Timeout, in seconds, to receive a reply to the EHLO/HELO command.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPHeloTimeout 300

SMTPMailFromTimeout [non-negative number]

Timeout, in seconds, to receive a reply to the MAIL FROM command.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPMailFromTimeout 300

SMTPRcptTimeout [non-negative number]

Timeout, in seconds, to receive a reply to the RCPT TO command.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPRcptTimeout 300

SMTPDataTimeout [non-negative number]

Timeout, in seconds, to receive a reply to the DATA command.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPDataTimeout 120

SMTPDataBlockTimeout [non-negative number]

Timeout, in seconds, for sending one data block.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPDataBlockTimeout 180

SMTPDataPeriodTimeout [non-negative number]

Timeout, in seconds, to receive a reply to the final dot

after sending the message.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

SMTPDataPeriodTimeout 600

```
# ----------------------------------------------------------------------
# MaxForwarders [non-negative number]
# Number of forwarders running simultaneously.
# (All the forwarders are of the same class, as specified by
# the following option).
#
# Default:
# MaxForwarders 10
# ----------------------------------------------------------------------
# ForwardTo [string]
# Select how mail should be forwarded.
# In milter mode this parameter will be used only for sending administrative
# mails.
#
# Send mail by piping it through sendmail (this is the default):
#
ForwardTo /usr/lib/sendmail -oem -oi
#
# Or if you want the mail to be sent by SMTP:
#
# ForwardTo SMTP: localhost port 825
#
# Default:
# ForwardTo "/usr/lib/sendmail -oem -oi"
```

```
# ------------------------------------------------------------------------
# ForwardTo2 [string]
# This option specifies the fallback forwarder that should be used
# if the primary forwarder (the one given in the ForwardTo option)
# failed to deliver mail. The syntax for this option is the same as the
# syntax for the ForwardTo option.
#
# This option is ignored if the primary forwarder or the fallback forwarder
# do not refer to an SMTP server.
#
# Whether the fallback forwarder will be used is determined by the outcome
# of a delivery attempt through the primary forwarder. If MailGate cannot
# establish a connection to the primary forwarder or if any SMTP command
# is answered with a 421 response or not answered at all (leading to a
# timeout) then another delivery attempt will be made using the fallback
# forwarder.
#
# Example:
# ForwardTo2 SMTP: smtp.example.com port 25
# ------------------------------------------------------------------------
# ScannerListenAddress [string]
# The location of the scanner's socket. MailGate connects
# to this socket to perform scan requests.
#
# IMPORTANT:
# If you change this option, you must also change the option
# "ListenAddress" in /etc/avira/avmailgate-scanner.conf.
#
```

Default:

ScannerListenAddress /var/run/avmailgate/scanner

MaxAttachments [non-negative number]

An email is classified as suspicious if it exceeds the maximum

attachment number.

Also see the BlockSuspiciousMime parameter.

#

Default:

MaxAttachments 100

BlockSuspiciousMime [boolean]

Stop delivery of suspicious MIME mails.

Whether or not emails are considered suspicious is influenced

by the MaxAttachments parameter.

#

Default:

BlockSuspiciousMime NO

BlockFragmentedMessage [boolean]

Block mails which are coded as a fragmented message.

"Message Fragmentation and Reassembly" (RFC2046, section 5.2.2.1).

#

Default:

BlockFragmentedMessage NO

```
# ------------------------------------------------------------------
# BlockPartialArchive [boolean]
# Block mails that contain an archive that
# is part of a multi volume archive.
#
# Default:
# BlockPartialArchive NO
# ------------------------------------------------------------------
# BlockExtensions [string]
# Block emails which have an attachment with one of the
# specified extensions in the filename.
# Each extension is separated by a semicolon.
# The maximum length for each extension is 120 characters.
#
# Note that filenames in archives are matched too, not
# only the name in the MIME header.
#
# Example:
# BlockExtensions exe;scr;pif
#
# Default:
# BlockExtensions NO
# ------------------------------------------------------------------
# ExposeRecipientAlerts [string]
# Send notifications about blocked mails to recipient(s)
#
# If ExposeRecipientAlerts is NO, no alerts will be sent to recipients.
# If ExposeRecipientAlerts is LOCAL, alerts to recipients will only be
```

sent if the recipient is local to your domain (local: in the .acl).

If ExposeRecipientAlerts is YES, alerts will always be sent to

recipients.

#

NOTE: LOCAL has no effect when running in milter mode.

#

Default:

ExposeRecipientAlerts YES

ExposeSenderAlerts [string]

Send notifications about blocked mails to the sender.

#

If ExposeSenderAlerts is NO, no alerts will be sent to the sender.

If ExposeSenderAlerts is LOCAL, alerts to the sender will only be

sent if the sender is local to your domain (local: in the .acl).

If ExposeSenderAlerts is YES, alerts will always be sent to

the sender.

#

NOTE: LOCAL has no effect when running in milter mode.

#

Default:

ExposeSenderAlerts NO

ExposePostmasterAlerts [boolean]

Send notifications about blocked mails to the postmaster.

#

Default:

ExposePostmasterAlerts YES

AlertsUser [string]

Sender address in notification mails.

#

Default:

AlertsUser AvMailGate

AddStatusInBody [string]

If AddStatusInBody is NO, no status notification is inserted in

the body of emails.

#

If AddStatusInBody is YES:

A default text will be inserted in each mail.

If a file named body-state exists in the template subdirectory

of the program directory, the text in this file will be inserted

in the mail (body-state is only used due to compatibility issues).

#

If AddStatusInBody is a full path to a file, the text in the given file

will be inserted in the mail.

#

Default:

AddStatusInBody NO

MaxMessageSizeStatus [size]

If AddStatusInBody is set, no status text will be inserted,

if the mail is larger than MaxMessageSizeStatus.

#

NOTE: values larger than 2000MB (2 GB) are not allowed.

```
#
# Example:
# MaxMessageSizeStatus 2MB
#
# Default:
# MaxMessageSizeStatus 0
# ------------------------------------------------------------------------
# ForwardAllEmailAsMIME [boolean]
# If ForwardAllEmailAsMIME is NO, incoming emails that are not MIME
# emails get out as they came, non-MIME.
#
# If ForwardAllEmailAsMIME is YES:
# The behaviour does not change for MIME emails.
# However, plain RFC mails will get a MIME header of Content-Type
# text/plain and Content-Disposition inline. The encoding is 7bit
# or 8bit depending on the original message.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# ForwardAllEmailAsMIME NO
# ------------------------------------------------------------------------
# ScanInArchive [boolean]
# If ScanInArchive is NO, no files in archives will be scanned.
#
# If ScanInArchive is YES, all files in archives will be extracted
# and scanned, depending on the restrictions given with
# ArchiveMaxSize, ArchiveMaxRecursion and ArchiveMaxRatio.
```

```
#
# Default:
ScanInArchive YES
# ----------------------------------------------------------------------
# ArchiveMaxSize [size]
# If ArchiveMaxSize is 0, all files in an archive will be extracted,
# don't care of their unpacked size.
#
# If ArchiveMaxSize is >0, all files up to the adjusted size will be
# extracted.
#
# Default:
ArchiveMaxSize 0
# ----------------------------------------------------------------------
# ArchiveMaxRatio [non-negative number]
# If the compression ratio is above the value specified here,
# the mail will not be scanned completely.
#
# If ArchiveMaxRatio is 0, the mail be scanned completely.
#
# Default:
ArchiveMaxRatio 150
# ----------------------------------------------------------------------
# ArchiveMaxRecursion [non-negative number]
# If ArchiveMaxRecursion is 0, recursive archives are going to be
# unpacked with an unlimited recursion depth.
#
# If ArchiveMaxRecursion is >0, recursive archives are going to be
```

```
# unpacked up to the adjusted recursion depth.
#
# Default:
ArchiveMaxRecursion 20
# ---------------------------------------------------------------------
# BlockSuspiciousArchive [boolean]
# If BlockSuspiciousArchive is NO, don't stop delivery of mails
# containing archives with suspicious content.
#
# If BlockSuspiciousArchive is YES, stop delivery of mails
# containing archives that reached the limits of ArchiveMaxRecursion,
# ArchiveMaxSize or ArchiveMaxRatio. Archives that couldn't be scanned
# completely will also be blocked if this option is enabled.
#
# Default:
# BlockSuspiciousArchive NO
# ---------------------------------------------------------------------
# BlockEncryptedArchive [boolean]
# If BlockEncryptedArchive is NO, don't stop delivery of mails
# containing encrypted files in archives.
#
# If BlockEncryptedArchive is YES, stop delivery of mails
# containing encrypted files in archives.
#
# Default:
# BlockEncryptedArchive NO
```

DetectADSPY [boolean]

Detect software that displays advertising pop-ups or software that very

often without the user's consent sends user specific data to

third parties and might therefore be unwanted.

#

Default:

DetectADSPY YES

DetectAPPL [boolean]

Detect applications of dubious origin or which might be hazardous to use.

#

Default:

DetectAPPL YES

DetectBDC [boolean]

Detect control software for backdoors. These are generally harmless.

#

Default:

DetectBDC YES

DetectDIAL [boolean]

Detect dial-up programs for connections that charge a fee. Its use might

lead to huge costs for the user.

#

Default:

DetectDIAL YES

DetectGAME [boolean]

Detect games that cause no damage on your computer.

#

Default:

DetectGAME NO

DetectHIDDENEXT [boolean]

Detect files that have an executable file extension but hide it

behind a harmless one.

#

Default:

DetectHIDDENEXT YES

DetectJOKE [boolean]

Detect harmless joke programs.

#

Default:

DetectJOKE NO

DetectPCK [boolean]

Detect files that have been compressed with an unusual runtime

compression tool. Please make sure that this file comes from a

trustworthy source.

#

Default:

DetectPCK YES

DetectPHISH [boolean]

Detect faked emails that are supposed to prompt the victim to reveal

confidential information such as user accounts, passwords or online-

banking data on certain websites.

#

Default:

DetectPHISH YES

DetectSPR [boolean]

Detect software that may be able to compromise the security of your system,

initiate unwanted program activities, damage your privacy or spy out

your user behaviour and might therefore be unwanted.

#

Default:

DetectSPR NO

HeuristicsMacro [boolean]

AntiVir is capable of using heuristics to determine if a file

may be malicious. This allows new or unknown malicious code to

be detected before you have had a chance to perform an update.

There are two types of heuristics that AntiVir uses. The

first, HeuristicsMacro, only deals with macros in office

documents. This can be disabled by setting HeuristicsMacro to "no".

#

Default:

HeuristicsMacro YES

```
# ------------------------------------------------------------------------
# HeuristicsLevel [non-negative number]
# Sets the intensity of the general heuristic scanner, which applies to
# all files. Valid values for this option are 0-3.
# 0 means disabled and 3 means full intensity.
#
# Default:
# HeuristicsLevel 3
# ------------------------------------------------------------------------
# BlockOnError [boolean]
# If BlockOnError is NO, don't stop delivery of mails
# containing archives that cause errors when processing them
# or that cause the scan process to timeout.
#
# If BlockOnError is YES, stop delivery of mails
# containing archives that cause errors when processing them
# or that cause the scan process to timeout.
#
# Default:
# BlockOnError NO
# ------------------------------------------------------------------------
# BlockUnsupportedArchive [boolean]
# If BlockUnsupportedArchive is NO, don't stop delivery of mails
# containing archives that can not be handled by the scanner.
#
# If BlockUnsupportedArchive is YES, stop delivery of mails
# containing archives that can not be handled by the scanner.
#
```

Default:

BlockUnsupportedArchive NO

RejectAlertMail [boolean]

If RejectAlertMail is YES, a mail containing an alert will be rejected

to the mail client with the message "Alert found in email".

It will be moved to the quarantine directory depending on the setting

QuarantineAlert.

#

If RejectAlertMail is NO, mail will be accepted and moved to the

quarantine directory.

#

NOTE: this option is only available when running in milter mode.

#

Default:

RejectAlertMail NO

QuarantineAlert [boolean]

If QuarantineAlert is YES and RejectAlertMail is YES, a mail

containing an alert will be rejected and the mail will be quarantined.

#

If QuarantineAlert is NO and RejectAlertMail is YES, the mail will be

rejected and will not be quarantined.

#

NOTE: this option is only available when running in milter mode.

#

Default:

QuarantineAlert YES

PollPeriod [non-negative number]

PollPeriod specifies the periodicity (in seconds) of the queue

scanning done by the forwarder/scanner process.

#

Default:

PollPeriod 60

QueueLifetime [timespan]

QueueLifetime specifies the maximum time a message can stay in the

queue before it will be bounced.

#

Note that MailGate will only check if the maximum lifetime has expired

everytime the forwarder is activated (that interval is set by the

ForwarderRetryDelay configuration option).

Thus it is recommended to set QueueLifetime to a multiple of

ForwarderRetryDelay.

#

0 disables this feature.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

QueueLifetime 0

ForwarderRetryDelay [timespan]

ForwarderRetryDelay specifies the maximum time between retrying

to send a queued message. Note that setting this value lower than

the PollPeriod parameter results in MailGate only trying to send

a queued message every PollPeriod seconds, i.e. the actual retry

timeout is the maximum of ForwarderRetryDelay and PollPeriod.

This setting is ineffective when running Avira MailGate in milter mode.

#

E.g. 30m

- The message will not be reprocessed within the next 30 minutes.

#

Default:

ForwarderRetryDelay 30m

ThrottleMessageCount [non-negative number]

ThrottleMessageCount is only needed if you have a huge queue and you do not

want the mails to be processed at once after starting the forwarder daemon.

Usually you do not need this option.

#

(Ineffective when running Avira MailGate in milter mode)

#

If this option and the option "ThrottleDelay" is set, only

"ThrottleMessageCount" mails will be reprocessed at once. After reprocessing

the mails, the forwarder daemon will sleep for "ThrottleDelay" seconds.

After "ThrottleDelay" seconds, the daemon will process the next

"ThrottleMessageCount" messages. This will be done until all messages

are reprocessed.

If the queue is empty this option will not be used anymore and throttling

will be disabled.

#

NOTE: If the queue gets filled during a throttled reprocessing of mails,

the new mails will not be processed immediately!

You should not accept mails while a throttled reprocessing of mails is active!

#

0 disables this feature.

#

Default:

ThrottleMessageCount 0

ThrottleDelay [non-negative number]

ThrottleDelay specifies the amount of seconds the forwarder daemon will

sleep after reprocessing "ThrottleMessageCount" queued mails.

See option "ThrottleMessageCount".

(Ineffective when running Avira MailGate in milter mode)

#

0 disables this feature.

#

Default:

ThrottleDelay 0

BounceMessageUser [string]

Sender address of bounce messages.

#

(Ineffective when running Avira MailGate in milter mode)

#

Default:

BounceMessageUser MAILER-DAEMON

```
# ------------------------------------------------------------------------
# BounceMessageSizeBody [size]
# BounceMessageSizeBody limits the size in bytes of the body of the original
# mail in the bounce mail.
# A value of 0 means unlimited.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# BounceMessageSizeBody 0
# ------------------------------------------------------------------------
# BounceMessageSizeHeader [size]
# BounceMessageSizeHeader limits the size in bytes of the header of the original
# mail in the bounce mail.
# A value of 0 means unlimited.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# BounceMessageSizeHeader 0
# ------------------------------------------------------------------------
# AddXHeader [boolean]
# If AddXHeader is YES, information about the scanning status is added
# to the header of the checked mail. E.g.: "X-AntiVirus: checked by ..."
#
# Default:
# AddXHeader YES
```

```
# ---------------------------------------------------------------------
# AddReceivedByHeader [boolean]
# If AddReceivedByHeader is YES, a "Received:" stamp is added to
# the header of the mail.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# AddReceivedByHeader YES
# ---------------------------------------------------------------------
# MaxHopCount [non-negative number]
# Prevent mail loops. If there are more than MaxHopCount "Received:"
# lines in the header, the mail will not be accepted.
# 0 disables this feature.
#
# (Ineffective when running Avira MailGate in milter mode)
#
# Default:
# MaxHopCount 100
# ---------------------------------------------------------------------
# ScanTimeout [non-negative number]
# Stop scanning if a scan takes longer than the given time in seconds.
#
# Default:
# ScanTimeout 300
```

```
# ---------------------------------------------------------------------
# ExternalProgram [string]
# Call external program or script if an alert was found. The first argument is
# the id of the rejected message.
#
# Example:
# ExternalProgram /dir/my_own_script
# ---------------------------------------------------------------------
# AlertAction [string]
# Action for alerts and suspicious mails.
#
# The available settings for this option are:
#  * QUARANTINE. Alerts and suspicious mails will be sent to quarantine.
#  * DELETE_ALERTS. Alerts will be deleted, but suspicious mails
#    will be quarantined.
#  * DELETE_ALL. Both alerts and suspicious mails will be deleted.
#
# Default:
# AlertAction QUARANTINE
# ---------------------------------------------------------------------
# NotifyEndOfLicense [non-negative number]
# Send a notification mail every day, 30 days before license will expire.
# 0 means no notification mail.
#
# Default:
NotifyEndOfLicense 30
```

AddPrecedenceHeader [string]

If AddPrecedenceHeader is YES, a line (Precedence: junk) is added to the

header of a notification mail. If neither YES nor NO is given, the custom text

will be inserted.

This option causes some E-Mail-autoresponders to NOT respond

to the received notification mail.

#

Default:

AddPrecedenceHeader NO

AddHeaderToNotice [boolean]

If AddHeaderToNotice is set to YES, the header of the rejected

mail will be appended to the postmaster notice mail.

#

Default:

AddHeaderToNotice YES

GuiSupport [boolean]

Enable GUI support.

#

Default:

GuiSupport NO

GuiCAFile [string]

Path to CA file.

#

```
# Default:
# GuiCAFile /usr/lib/AntiVir/mailgate/gui/cert/cacert.pem
# ----------------------------------------------------------------------
# GuiCertFile [string]
# Path to cert file.
#
# Default:
# GuiCertFile /usr/lib/AntiVir/mailgate/gui/cert/server.pem
# ----------------------------------------------------------------------
# GuiCertPass [string]
# Password for certificate.
#
# Default:
# GuiCertPass antivir_default
# ----------------------------------------------------------------------
# GuiRandFile [string]
# Path to random file.
# Do not use an endless file like /dev/random or /dev/urandom.
#
# Example:
# GuiRandFile /path/to/file
# ----------------------------------------------------------------------
# EnableSpamCheck [boolean]
# Check mails for spam, suspicious and dangerous content.
#
# Default:
# EnableSpamCheck NO
```

```
# ------------------------------------------------------------------------
# SpamAction [string]
# Action for spam mails.
#
# NONE disables any action for spam mails.
#
# TAG inserts a header line into the mail:
#X-AntiVirus-Spam-Check: spam (checked by ...)
#
# BLOCK quarantines the mail to the "rejected" directory.
#
# See /usr/lib/AntiVir/mailgate/antivir_mailgate_en.txt for more details.
#
# Default:
# SpamAction TAG
# ------------------------------------------------------------------------
# DangerousOutbreakAction [string]
# Action for dangerous outbreaks.
#
# NONE disables any action for dangerous outbreaks.
#
# TAG inserts a header line into the mail:
#  X-AntiVirus-Spam-Check: dangerous outbreak (checked by ...)
#
# BLOCK quarantines the mail to the "rejected" directory.
#
# See /usr/lib/AntiVir/mailgate/antivir_mailgate_en.txt for more details.
#
```

Default:

DangerousOutbreakAction BLOCK

DangerousAttachmentAction [string]

Action for dangerous attachments.

#

The attachments are identified by their suffix:

.ade .adp .bas .bat .bhx .ceo .cer .chm .cmd .com .cpl

.crt .exe .hlp .hta .inf .ins .isp .js .jse .lnk .mde .mim

.msc .msi .msp .mst .ole .pcd .pi .pif .reg .scr .sct .shb

.shs .vb .vbe .vbs .wmd .wmz .wsc .wsf .wsh .xxe

#

NONE disables any action for dangerous attachments.

#

TAG inserts a header line into the mail:

X-AntiVirus-Spam-Check: dangerous attachment (checked by ...)

#

BLOCK quarantines the mail to the "rejected" directory.

#

Default:

DangerousAttachmentAction TAG

DangerousIFrameAction [string]

Action for dangerous iFrames.

#

NONE disables any action for dangerous iFrames.

#

TAG inserts a header line into the mail:

```
#  X-AntiVirus-Spam-Check: dangerous iframe (checked by ...)
#
# BLOCK quarantines the mail to the "rejected" directory.
#
# Default:
# DangerousIFrameAction TAG
# ------------------------------------------------------------------
# DangerousAlertAction [string]
# Action for dangerous alerts.
#
# NONE disables any action for dangerous alerts.
#
# TAG inserts a header line into the mail:
#  X-AntiVirus-Spam-Check: dangerous alert (checked by ...)
#
# BLOCK quarantines the mail to the "rejected" directory.
#
# Default:
# DangerousAlertAction BLOCK
# ------------------------------------------------------------------
# DangerousUnknownAction [string]
# Action for dangerous unknown.
#
# NONE disables any action for dangerous unknown.
#
# TAG inserts a header line into the mail:
#  X-AntiVirus-Spam-Check: dangerous unknown (checked by ...)
#
```

```
# BLOCK quarantines the mail to the "rejected" directory.
#
# Default:
# DangerousUnknownAction TAG
# ------------------------------------------------------------------------
# LibAsmailgate [string]
# Path to spam filter library.
#
# Default:
# LibAsmailgate /usr/lib/AntiVir/mailgate/libasmailgate.so
# ------------------------------------------------------------------------
# SpamHeaderName [string]
# Set custom X-header key instead of X-AntiVirus-Spam-Check.
# The string must conform to RFC 2822.
# The value for the custom key cannot be customized.
#
# Default:
# SpamHeaderName X-AntiVirus-Spam-Check
# ------------------------------------------------------------------------
# SpamFilterExceptions [string]
# Spam filter list of exceptions for black/white lists and
# actions.
#
# See /usr/lib/AntiVir/mailgate/antivir_mailgate_en.txt for details about
# the exception file.
#
# Default:
# SpamFilterExceptions /etc/avira/asmailgate.except
```

SpamFilterDetectGTUBE [boolean]

The GTUBE test string can be used to test the integrated spam filter.

The string and a complete RFC-822 mail can be found here:

http://spamassassin.apache.org/gtube/

#

Default:

SpamFilterDetectGTUBE NO

SpamFilterStartupTimeout [non-negative number]

This option specifies how long Avira MailGate shall wait for the external

spam daemon to come up (in seconds).

#

Default:

SpamFilterStartupTimeout 60

SpamFilterServiceConnectTimeout [non-negative number]

This option specifies how long Avira MailGate shall wait for an

answer of a configuration request to the external

spam filter daemon (in seconds).

#

Default:

SpamFilterServiceConnectTimeout 30

SpamFilterServiceMaxSessions [non-negative number]

This option sets the maximum limit of simultaneous running

threads of the external spam filter daemon.

#

```
# Default:
# SpamFilterServiceMaxSessions 50
# ------------------------------------------------------------------
# SpamFilterHandleBulkADVLikeSpam [boolean]
# Rate category bulk advertisement as spam.
#
# Default:
# SpamFilterHandleBulkADVLikeSpam NO
# ------------------------------------------------------------------
# SpamFilterHandleBulkPornLikeSpam [boolean]
# Rate category bulk porn as spam.
#
# Default:
# SpamFilterHandleBulkPornLikeSpam NO
# ------------------------------------------------------------------
# SpamFilterModifySubject [boolean]
# Add the spam check result to the original Subject: header line.
# (Subject: [spamcheck: spam] this is the original subject text)
#
# If the template file <AntiVirDir>/templates/spamfilter-subjects
# exists, the strings specified in the template will be
# used as replacement.
#
# A sample template can be found in <AntiVirDir>/templates/examples/spamfilter-subjects
# The file consists of lines that will be used as replacements:
# <spam check result> <custom string|keywords>
#
# E. g.:
```

Spam ***SPAM*** %SUBJECT%

This will result in a replaced "Subject:" header line like:

Subject: ***SPAM*** original subject

#

Please see the template file for details.

#

Default:

SpamFilterModifySubject NO

SpamFilterCheckFailedKeep [boolean]

Requeue a mail if the spam check failed.

The mail will be put back to the queue to be reprocessed later. It

will be reprocessed as long as the error persists.

#

NOTE: At the moment you can't enforce the delivery of a mail that is stuck

in the queue.

#

Default:

SpamFilterCheckFailedKeep NO

OpenMax [number]

Specify the maximum number of opened files

for the Avira MailGate processes.

#

If the value given here is less than 1, then MailGate will ensure

that at least 1024 files can be opened at any time.

#

If the value specified here is greater than 0, MailGate will set

the maximum number of opened files to this value.

#

Usually it is not necessary to change this value.

#

Default:

OpenMax 1024

DBSupport [boolean]

Database support.

#

If this option is enabled, MailGate writes statistics information to a database.

Please refer to /usr/lib/AntiVir/mailgate/antivir_mailgate_en.txt for more

information about the database support.

#

Default:

DBSupport NO

DBodbcIni [string]

Database odbc.ini file.

#

The ODBC driver manager will use the specified odbc.ini.

#

Default: It's left to the installed ODBC driver manager which odbc.ini

file it loads.

#

Example:

DBodbcIni /path/to/odbc.ini

```
# ----------------------------------------------------------------------
# DBodbcLib [string]
# Database odbc driver manager.
#
# MailGate will load the specified library and use it as the
# ODBC driver manager.
#
# Default:
#     Load one of the following libraries from the default library path
#     in this order:
#
#     libodbc.so.1
#     libodbc.so
#     libiodbc.so
#
# Example:
# DBodbcLib /path/to/odbc-library
# ----------------------------------------------------------------------
# DBodbcDataSource [string]
# Database source name.
#
# Connect to the given database source.
#
# Default:
# DBodbcDataSource MailGate
```

--

DBUpdateDelay [timespan]

Database update delay for counters.

#

Wait this delay before writing the next summed up counters to the

database.

#

Default: Write counters to database every full hour.

#

Default:

DBUpdateDelay 1h

--

DBStoreAlertsForEachRecipient [boolean]

How many rows to write to the alerts table per mail.

#

If this option is enabled, there will be one row in the alerts table

for each recipient of a mail. If it's disabled, there will only be

one row per mail (which will mention the first recipient).

#

Default: Only write one row per mail to the alerts table.

#

Default:

DBStoreAlertsForEachRecipient NO

--

DBLogCleanMails [boolean]

Log information about clean mails to the database.

#

This option specifies if information about clean mails will

be written to the database.

The fields "reason", "queueid", "action", "source", "product", "vdf",

"engine", ("ou"), and "date" will be set for clean mails.

"reason" will be set to "Clean" and "action" to "processed".

#

Default:

DBLogCleanMails NO

LogAlertsForEachRecipient [boolean]

How many log entries to generate per mail.

#

If this option is enabled, there will be one log entry

for each recipient of a mail. If it's disabled, there will only be

one log entry per mail (which will mention the first recipient).

#

Default:

LogAlertsForEachRecipient NO

ActiveDirectorySupport [boolean]

Active Directory support.

#

If this option is enabled, MailGate will query the specified

Active Directory server for mails' recipients addresses.

If the addresses are found in the directory, the first

organizational unit that the address belongs to is associated

with the recipient and included in following log messages resp.

database records.

MailGate doesn't have a maximum length for the organizational unit

names.

#

Note that this feature depends on the IPv4 protocol being

enabled (see config option InetProtocols).

#

Default:

ActiveDirectorySupport NO

ActiveDirectoryServerURI [string]

Active Directory server(s) to use.

#

Specifies the Active Directory server(s) to use for recipient lookups.

The use of the protocol prefix (ldap://) is mandatory, you may omit

the port number though.

You may specify more than one URL (delimited by spaces) in this

configuration option. In that case, MailGate will use the first of the given

servers that it can connect to.

#

Alternatively, you can specify a single absolute filename in this config

option. In this case, a list of mappings from email addresses to group names

is read from the given file, and no Active Directory server is needed.

See avmailgate.groups for an example file.

#

Note that it's not possible to specify both a filename and one or more

Active Directory server URIs.

#

Example:

ActiveDirectoryServerURI ldap://my.ad-server.com:389

```
# Default:
# ActiveDirectoryServerURI ""
# ----------------------------------------------------------------------
# ActiveDirectoryBaseDN [string]
# The distinguished name of the Active Directory entry at which
# searches will be started.
#
# Setting this config option to a valid Active Directory entry
# is mandatory.
#
# Example:
# ActiveDirectoryBaseDN dc=example,dc=com
#
# Default:
# ActiveDirectoryBaseDN ""
# ----------------------------------------------------------------------
# ActiveDirectoryLogin [string]
# The distinguished name of the Active Directory entry that is used to
# log into the Active Directory server.
#
# If this option is unset/empty, MailGate will issue anonymous
# Active Directory queries. Note that your Active Directory server might
# not allow anonymous queries though (in this case, the queries will fail).
#
# Example:
# ActiveDirectoryLogin cn=Administrator,cn=Users,dc=mail,dc=example,dc=com
#
```

Default:

ActiveDirectoryLogin ""

ActiveDirectoryPassword [string]

The password for the user specified by the ActiveDirectoryLogin

config value.

#

This option has no effect if ActiveDirectoryLogin is unset/empty.

#

Example:

ActiveDirectoryPassword secret

#

Default:

ActiveDirectoryPassword ""

ActiveDirectoryUseTLS [boolean]

If this option is enabled, MailGate will use TLS encryption for the

Active Directory connections.

#

Note that you also need to set the ActiveDirectoryCACertificates

option to be able to use TLS.

#

Default:

ActiveDirectoryUseTLS NO

ActiveDirectoryCACertificates [string]

This config option is set to the path of the file that contains the

certificates of all certificate authorities that are accepted by MailGate.

Example:

ActiveDirectoryCACertificates /etc/avira/active_directory_cas.crt

----

ActiveDirectorySASLAuthMechanism [string]

The SASL authentication mechanism that should be used to

authenticate to the Active Directory server.

#

The supported values for this option are PLAIN and DIGEST-MD5.

#

Note that when using the PLAIN authentication mechanism,

your password will be transmitted to the server in clear text.

This is a security problem, since a third party that is able

to read your network traffic could also intercept your

login credentials.

#

Thus it is strongly recommended that PLAIN only be used

in combination with TLS (see ActiveDirectoryUseTLS).

#

Note also that the DIGEST-MD5 authentication mechanism might

not work if you are trying to login with the administrator

account.

#

Example:

ActiveDirectorySASLAuthMechanism DIGEST-MD5

#

Default:

ActiveDirectorySASLAuthMechanism PLAIN

ActiveDirectorySearchTimeout [non-negative number]

The timeout to use for Active Directory searches. Given in milliseconds.

#

Default:

ActiveDirectorySearchTimeout 30000

ActiveDirectoryBindTimeout [non-negative number]

The timeout to use for Active Directory logins (bind operations).

Given in milliseconds.

#

Default:

ActiveDirectoryBindTimeout 5000

ActiveDirectoryCacheSize [non-negative number]

Active Directory search cache size.

#

Specifies how many Active Directory search results should be cached

by MailGate.

#

Default:

ActiveDirectoryCacheSize 1024

ActiveDirectoryCacheTTL [timespan]

Specifies for how long Active Directory search results

will be cached. This option is ineffective if ActiveDirectoryCacheSize

is zero.

#

Default:

ActiveDirectoryCacheTTL 30m

ActiveDirectoryCheckUserAccountControl [boolean]

If enabled, MailGate will inspect the userAccountControl attribute

of Active Directory entries to determine whether the account is active

or not. Only entries whose userAccountControl attribute has bit two

set are considered active in this case.

#

Default:

ActiveDirectoryCheckUserAccountControl YES

ActiveDirectoryGroupBlackList [string]

Using this config option, you may control which organizational unit

names get written to the database. It has no effect on the outcome

of the recipient validity check that is done if RejectUnknownRecipients

is enabled.

#

The value of this option is a semicolon-delimited list of distinguished

names of organizational units that are to be ignored in recipient

lookups. Organizational units listed here will not be logged/stored in

the database.

#

The black list is overridden by the white list, i.e. if the

ActiveDirectoryGroupWhiteList option is used, the value of

ActiveDirectoryGroupBlackList is ignored.

#

Example:

```
# ActiveDirectoryGroupBlackList FirstDN; SecondDN
#
# Default:
# ActiveDirectoryGroupBlackList ""
# ------------------------------------------------------------------
# ActiveDirectoryGroupWhiteList [string]
# Using this config option, you may control which organizational unit
# names get written to the database. It has no effect on the outcome
# of the recipient validity check that is done if RejectUnknownRecipients
# is enabled.
#
# The value of this option is a semicolon-delimited list of distinguished
# names of organizational units that are allowed in recipient lookups.
# Only organizational units listed here will be logged/stored in the database.
#
# The white list overrides the black list, i.e. if this config option
# is used, the value of ActiveDirectoryGroupBlackList is ignored.
#
# Example:
# ActiveDirectoryGroupWhiteList FirstDN; SecondDN
#
# Default:
# ActiveDirectoryGroupWhiteList ""
# ------------------------------------------------------------------
# RejectUnknownRecipients [boolean]
# Reject emails that are addressed at users which are not contained
# in the Active Directory. This option is only respected if the
# ActiveDirectorySupport option is enabled.
```

```
#
# Default:
# RejectUnknownRecipients NO
# ------------------------------------------------------------------
# NotificationMechanisms [string]
# The semicolon separated list of transports that should be used to
# send notifications to the postmaster/administrator.
# These notifications are sent in case of errors or other situations
# that usually require the administrator's attention.
#
# The supported mechanisms are:
# EMAIL - the postmaster account is sent mail describing the problem
# SNMP  - an SNMP trap is sent (depends on SNMPRecipient being set, too).
#         Note that the SNMP mechanism depends on the IPv4 protocol being
#         enabled (see config option InetProtocols).
#
# To disable this feature, set the config option to NONE.
#
# Example:
# NotificationMechanisms mechanism1 ; mechanism2
#
# Default:
# NotificationMechanisms EMAIL
# ------------------------------------------------------------------
# SNMPRecipient [string]
# The name of the host to which SNMP traps should be sent.
# May optionally be followed by a colon and a port number.
#
```

Note that this setting takes effect only if the SNMP notification

mechanism has been enabled.

#

Example:

SNMPRecipient localhost:162

#

Default:

SNMPRecipient ""

SNMPSender [string]

This option is used to specify the network interface that will be stored

in SNMP traps as the traps' originating IP address.

#

Valid values are IPv4 addresses or hostnames.

By default, MailGate will use the IP address that the value of the

MyHostName config option resolves to.

#

Note that this setting takes effect only if the SNMP notification

mechanism has been enabled.

#

Example:

SNMPSender 192.168.1.100

SNMPCommunity [string]

SNMP aware applications can by grouped by means of community membership.

By default, Avira MailGate belongs to the Avira community.

The maximum length for the string provided for this option is 255 characters.

#

Note that this setting takes effect only if the SNMP notification

mechanism has been enabled.

#

Default:

SNMPCommunity Avira

EncryptedEmailAction [string]

How to react to encrypted MIME emails.

#

If MailGate finds an encrypted MIME email in the incoming queue,

it will take the action given here.

#

Supported actions are IGNORE, NOTIFY_POSTMASTER and TREAT_AS_SUSPICIOUS.

Only one of these actions may be specified.

If the IGNORE action is enabled, encrypted MIME emails will just be

forwarded to the recipients.

If the NOTIFY_POSTMASTER action is enabled, a notification will be

emailed to the postmaster (the encrypted MIME email will still be

forwarded to the recipients).

If the TREAT_AS_SUSPICIOUS action is enabled, encrypted MIME emails

will be treated as suspicious and will not be delivered.

#

Default:

EncryptedEmailAction IGNORE

```
# ------------------------------------------------------------------------
# InetProtocols [string]
# The semicolon delimited list of internet protocols that can be used
# by MailGate.
#
# The supported protocols are:
# IPv4 - version four of the internet protocol
# IPv6 - version six of the internet protocol
#
# You may use this config option to enable a single protocol,
# or to enable both protocols.
# Note that the following features of MailGate require IPv4;
# they won't work if you disable the use of IPv4 using this config option.
#
# These features are:
# Milter mode
# ActiveDirectory support
# SNMP support
#
# Example:
# InetProtocols IPv4 ; IPv6
#
# Default:
# InetProtocols IPv4
```

```
# ---------------------------------------------------------------------
# UsePipeliningInSMTPClient [boolean]
# This config option controls whether or not MailGate should make use
# of the command pipelining SMTP extension (RFC 2920) in its SMTP client.
#
# This option has no effect unless an SMTP server is configured as your
# forwarder (via config option ForwardTo) and that server supports the
# command pipelining SMTP extension.
#
# If these prerequisites are fulfilled, enabling pipelining can
# improve mail delivery speed, especially if the forwarder SMTP server
# does not run on the same system as MailGate.
#
# Default:
# UsePipeliningInSMTPClient NO
# ---------------------------------------------------------------------
# IncomingHighFillLevel [non-negative number]
# MailGate will stop accepting new connections to its SMTP server once
# there are this many mails in the incoming queue. However, depending on
# the performance and load of the system, MailGate might allow the number
# of mails to slightly exceed the high fill level.
#
# MailGate will only accept new connections again once the number of mails
# in the incoming queue has reached the value of IncomingLowFillLevel again.
#
# Note that after restarting MailGate, MailGate will accept new mails again
# even if the number of mails in the incoming queue is higher than
# IncomingLowFillLevel but lower than IncomingHighFillLevel.
```

Setting this value to zero disables this feature.

#

Default:

IncomingHighFillLevel 0

IncomingLowFillLevel [non-negative number]

See the documentation for IncomingHighFillLevel.

#

Default:

IncomingLowFillLevel 0

OutgoingHighFillLevel [non-negative number]

MailGate will stop accepting new connections to its SMTP server once

there are this many mails in the outgoing queue. However, depending on

the performance and load of the system, MailGate might allow the number

of mails to slightly exceed the high fill level.

#

MailGate will only accept new connections again once the number of mails

in the outgoing queue has reached the value of OutgoingLowFillLevel again.

#

Note that after restarting MailGate, MailGate will accept new mails again

even if the number of mails in the outgoing queue is higher than

OutgoingLowFillLevel but lower than OutgoingHighFillLevel.

#

Setting this value to zero disables this feature.

#

Default:

OutgoingHighFillLevel 0

OutgoingLowFillLevel [non-negative number]

See the documentation for OutgoingHighFillLevel.

#

Default:

OutgoingLowFillLevel 0

8.8 /etc/avira/avmailgate.acl

Avmailgate.acl

Access lists for Avira MailGate

These hosts and/or domains are local.

local: localhost

local: relais.bbs.fh-wilhelmshaven.de

These hosts and networks are allowed to relay.

Relay: 10.0.0.1/8 127.0.0.1/8 192.168.0.0/16

8.9 /etc/avira/groups

avmailgate.groups

This file contains mappings of email addresses to group names using

(perl compatible) regular expressions.

Lines starting with the hash symbol (#) are ignored.

#

In this file each line starts with the keyword "grp", followed by

a space, a perl compatible regular expression, followed by a space,

and a group name. The group name is associated with all addresses that

match the given regular expression.

#

For example, the following line maps all addresses that start with

'person' followed by one or more numbers followed by '@example.com'

to the group 'groupOne'.

grp /^person\d+@example.com$/ groupOne

8.10 /etc/avira/avmailgate.ignore

avmailgate.ignore

This file is used to handle

the scanning of E-Mails based

on their sender and/or recipient

addresses.

#

For more detailed information

of this file please read the

MANUAL included in this package.

#

The syntax is perl compatible

regular expression.

#

This will not scan a mail to

virus@mydomain.tld :

#

/^virus@mydomain\.tld$/

8.11 /etc/avira/avmailgate-odbc.ini

avmailgate-odbc.ini
; This is an example odbc.ini file.

; Please see Avira MailGate's MANUAL and your

; ODBC driver manager's documentation for details.

;[MailGate]

;Driver = /path/to/driver-lib

;Server = server

;User = username

;Password = password

;Database = database

8.12 /etc/avira/avmailgate.scan

avmailgate.scan

This file is used to handle

the scanning of E-Mails based

on their sender and/or recipient

addresses.

#

For more detailed information

of this file please read the

MANUAL included in this package.

#

The syntax is perl compatible

regular expression.

#

The following scans every mail:

#

/.*/

8.13 /etc/avira/avmailgate-scanner.conf

avmailgate-scanner.conf

This is MailGate's scanner backend configuration file.

It is used to set values for scanner specific

options.

ListenAddress [address]

#

The socket on which the scanner will listen for scan requests.

#

IMPORTANT:

#

When changing this option, you also have to change the option

"ScannerListenAddress" in MailGate's configuration file

(default /etc/avira/avmailgate.conf).

ListenAddress unix:/var/run/avmailgate/scanner

SocketPermissions [mode]

#

The permissions of the scanner backend's socket.

SocketPermissions 0600

```
# ------------------------------------------------------------------
# User [user]
#
# The user the scanner runs as.
#
# IMPORTANT:
#
# When changing this option, you also have to change the option
# "User" in MailGate's configuration file
# (default /etc/avira/avmailgate.conf). Changing this option has several
# side effects with MailGate. You have to make sure that all
# directories and files are still accessible to this user.
# Please see the file "MANUAL" in the package for details.
User uucp
# ------------------------------------------------------------------
# Group [group]
#
# The group the scanner runs as.
#
# IMPORTANT:
#
# When changing this option, you also have to change the option
# "Group" in MailGate's configuration file
# (default /etc/avira/avmailgate.conf). Changing this option has several
# side effects with MailGate. You have to make sure that all
# directories and files are still accessible to this user.
# Please see the file "MANUAL" in the package for details.
Group antivir
```

```
# ------------------------------------------------------------------
# PoolScanners [integer]
#
# SAVAPI uses a pool of scanners to perform scans more efficiently,
# and this option is used to control how many scanners SAVAPI will put
# in the pool on startup.
#
# While this pool increases throughput this feature requires the pool
# size to be wisely chosen -- too many scanners will put load on the
# machine without gaining more performance, too few scanners may
# have the SAVAPI using applications wait unnecessarily.
#
# Default: PoolScanners 24
# ------------------------------------------------------------------
# PoolConnections [integer]
#
# The maximum number of simultaneous allowed connections
# from Avira MailGate to the scanner pool.
#
# Default: PoolConnections 128
# ------------------------------------------------------------------
# SyslogFacility [facility]
#
# The facility that is used to when logging to syslog.
SyslogFacility mail
# ------------------------------------------------------------------
# LogFileName [path]
#
```

The path to a filename to which SAVAPI will write log messages

(in addition to syslog, if enabled). Note that SAVAPI must be able

to access the file when running as the specified User/Group.

#

Default: LogFileName NONE

--

ReportLevel [integer]

#

The report level sets the log verbosity of the scanner backend.

Available values:

#

0 Log errors

1 Log errors and alerts

2 Log errors, alerts and warnings

3 Log errors, alerts, warnings and debug messages

#

("alerts" is information about potential malicious code).

#

Default: ReportLevel 0

--

ScanTemp [path]

#

The directory used by the scanner to store temporary files like

extracted files from archives.

It's also used for other temporary files like lock files.

#

NOTE:

#

```
# The scanner backend does not recognize the environment variable
# "TMPDIR".
#
# IMPORTANT:
#
# You may want to change the option "TemporaryDir" in MailGate's
# configuration file (default /etc/avira/avmailgate.conf) to set a
# proper location for processing mails.
# (You can use the same value for both parameters).
#
# Default: ScanTemp /var/tmp
```

8.14 /etc/avira/avmailgate.warn

```
avmailgate.warn
# This file is used to specify whether and how warnings
# are sent depending on the alert.
#
# For versions >= 2.0.2-X
# the syntax is perl compatible
# regular expression.
#
# For versions < 2.0.2-X
# wildcards have to be used.
# (e.g. *eicar*).
#
# E.g.: if an eicar testvirus
#       was found in an email
```

only the recipient

and the postmaster

will get a notice mail.

#

/eicar/i RP

8.15 /etc/avira/avupdate-mailgate.conf

avupdater-mailgate.conf

Please DO NOT CHANGE this file. If yes, you do it on your own responsibility.

The list of Internet update servers.

internet-srvs=http://dl1.pro.antivir.de,http://dl2.pro.antivir.de,http://dl3.pro.antivir.de,http://dl1.antivir.net,http://dl2.antivir.net,http://dl3.antivir.net

Specifies the master.idx file.

master-file=/idx/master.idx

Specifies the installation directory for updated product files.

install-dir=/usr/lib/AntiVir

Temporary directory for downloading updates.

temp-dir=/tmp/avira_update/mailgate

#The method for sending mails. Can have one of the following values:

smtp - for using own smtp engine

sendmail - for using sendmail binary

#mailer=

The smtp server for sending email notifications.

smtp-server=localhost

The smtp port for sending email notifications.

smtp-port=25

If auth-method is set, the Updater requires the smtp login data

```
#smtp-user=

#smtp-password=

# When set, the Updater requires the smtp login data: smtp-user and smtp-password

#auth-method=

# If the machine uses a HTTP proxy server, proxy configuration settings

# must be specified in order to make internet updates.

# The name of the proxy server.

proxy-host=10.1.0.1

# The port the proxy server listens on.

proxy-port=8080

# Username for proxy authentication.

proxy-username=super

# Password for proxy authentication.

proxy-password=antivir

# Option for setting the event types which cause the Updater to send emails:

# - 0 - no email notifications are sent.

# - 1 - email notifications are sent in case of "successful update", "unsuccessful

#       update", or "up to date".

# - 2 - email notification only in case of "unsuccessful update".

# - 3 - email notification only in case of "successful update".

notify-when=2

# Receiver of the notification emails.

email-to=root@localhost

# Full path for the Updater's log file.

# Note:

# If this option is not present, a default logfile with the name 'avupdate.log'

# will be created in the same directory as the updater binary.

log=/var/log/avupdate-mailgate.log
```

Overwrite logfiles by rotation (This parameter is mutual exclusive with log-append).

#log-rotate

Append messages to log file (By default, the log is overwritten).

log-append

8.16 /etc/avira/asmailgate.exept

This file is used by Avira MailGate to overwrite

default configuration settings for the spam filter

and to provide black and whitelisting of email addresses

for the spam filter.

#

NOTE: asmailgate.except is only used for the spam filter.

The black and whitelisting does _not_ affect the regular

scan procedure for malware.

#

The format of this file is:

/regular expression/ <action> ...

#

Example:

/^someone@somewhere\.tld$/i blacklist

#

The above example treats mails from someone@somewhere.tld as spam,

independently of the spam check result.

"blacklist" is the action for the given address.

#

The following actions are available:

#

blacklist - Treat mail as spam

whitelist - Treat mail as clean

#

block_spam - If the mail is spam, block it

block_dangerous_attachment - If the mail has a dangerous attachment, block it

block_dangerous_alert - If the mail contains a dangerous alert, block it

block_dangerous_iframe - If the mail contains a dangerous iframe, block it

#

tag_spam - If the mail is spam, tag it

tag_dangerous_attachment - If the mail has a dangerous attachment, tag it

tag_dangerous_alert - If the mail contains a dangerous alert, tag it

tag_dangerous_iframe - If the mail contains a dangerous iframe, tag it

#

NOTE: *_dangerous_outbreak is not available as an exception

since it is too sensitive to be used in exceptions.

Please use the option "DangerousOutbreakAction" in avmailgate.conf

to change the behaviour for dangerous outbreaks globally.

#

Actions can also be switched off.

#

Example:

/etc/avira/avmailgate.conf:

SpamAction BLOCK

#

/etc/avira/asmailgate.except:

/^me@here\.tld$/i r !block_spam

#

Do not block spam for the given recipient address.

```
#
# Did you notice the "r"?
# "r" is the flag for recipient. It means that the given address should be
# matched against the recipient address and not against the sender
# address.
# The default (without the "r" flag) is to match the address
# against the sender address.
#
# Another example:
# /etc/avira/avmailgate.conf:
# DangerousAttachmentAction TAG
#
# /etc/asmailgate.except:
# /^me@here\.tld$/i r !tag_dangerous_attachment !tag_dangerous_iframe
#
# Don't tag DangerousAttachment and DangerousIFrame mails.
```

8.17 /etc/aliases

```
#
#  Aliases in this file will NOT be expanded in the header from
#  Mail, but WILL be visible over networks or from /bin/mail.
#
#          >>>>>>>>>>   The program "newaliases" must be run after
#          >> NOTE >>   this file is updated for any changes to
#          >>>>>>>>>>   show through to sendmail.
#
# Basic system aliases -- these MUST be present.
```

mailer-daemon: postmaster

postmaster: root

General redirections for pseudo accounts.

bin: root

daemon: root

adm: root

lp: root

sync: root

shutdown: root

halt: root

mail: root

news: root

uucp: root

operator: root

games: root

gopher: root

ftp: root

nobody: root

radiusd: root

nut: root

dbus: root

vcsa: root

canna: root

wnn: root

rpm: root

nscd: root

pcap: root

apache: root

webalizer: root

dovecot: root

fax: root

quagga: root

radvd: root

pvm: root

amanda: root

privoxy: root

ident: root

named: root

xfs: root

gdm: root

mailnull: root

postgres: root

sshd: root

smmsp: root

postfix: root

netdump: root

ldap: root

squid: root

ntp: root

mysql: root

desktop: root

rpcuser: root

rpc: root

nfsnobody: root

ingres: root

system: root

toor: root

manager: root

dumper: root

abuse: root

newsadm: news

newsadmin: news

usenet: news

ftpadm: ftp

ftpadmin: ftp

ftp-adm: ftp

ftp-admin: ftp

www: webmaster

webmaster: root

noc: root

security: root

hostmaster: root

info: postmaster

marketing: postmaster

sales: postmaster

support: postmaster

trap decode to catch security attacks

decode: root

Person who should get root's mail

#root: linnemann@bbs.fh-wilhelmshaven.de

root: s103058@bbs.fh-wilhelmshaven.de

8.18 /etc/mail/sendmail.cf

```
#
# Copyright (c) 1998-2004 Sendmail, Inc. and its suppliers.
#       All rights reserved.
# Copyright (c) 1983, 1995 Eric P. Allman.  All rights reserved.
# Copyright (c) 1988, 1993
#       The Regents of the University of California.  All rights reserved.
#
# By using this file, you agree to the terms and conditions set
# forth in the LICENSE file which can be found at the top level of
# the sendmail distribution.
#
#
##########################################################################
##########################################################################
#####
#####             SENDMAIL CONFIGURATION FILE
#####
##### built by root@relais on Do 12. Apr 12:35:13 CEST 2012
##### in /etc/mail
##### using /usr/share/sendmail-cf/ as configuration include directory
#####
##########################################################################
#####
#####   DO NOT EDIT THIS FILE!  Only edit the source .mc file.
#####
##########################################################################
```

```
##########################################################################
#####  $Id: cfhead.m4,v 8.116 2004/01/28 22:02:22 ca Exp $  #####
#####  $Id: cf.m4,v 8.32 1999/02/07 07:26:14 gshapiro Exp $  #####
#####  setup for linux  #####
#####  $Id: linux.m4,v 8.13 2000/09/17 17:30:00 gshapiro Exp $  #####
#####  $Id: local_procmail.m4,v 8.22 2002/11/17 04:24:19 ca Exp $  #####
#####  $Id: no_default_msa.m4,v 8.2 2001/02/14 05:03:22 gshapiro Exp $  #####
#####  $Id: smrsh.m4,v 8.14 1999/11/18 05:06:23 ca Exp $  #####
#####  $Id: mailertable.m4,v 8.25 2002/06/27 23:23:57 gshapiro Exp $  #####
#####  $Id: virtusertable.m4,v 8.23 2002/06/27 23:23:57 gshapiro Exp $  #####
#####  $Id: redirect.m4,v 8.15 1999/08/06 01:47:36 gshapiro Exp $  #####
#####  $Id: always_add_domain.m4,v 8.11 2000/09/12 22:00:53 ca Exp $  #####
#####  $Id: use_cw_file.m4,v 8.11 2001/08/26 20:58:57 gshapiro Exp $  #####
#####  $Id: use_ct_file.m4,v 8.11 2001/08/26 20:58:57 gshapiro Exp $  #####
#####  $Id: local_procmail.m4,v 8.22 2002/11/17 04:24:19 ca Exp $  #####
#####  $Id: access_db.m4,v 8.26 2004/06/24 18:10:02 ca Exp $  #####
#####  $Id: blacklist_recipients.m4,v 8.13 1999/04/02 02:25:13 gshapiro Exp $  #####
#####  $Id: accept_unresolvable_domains.m4,v 8.10 1999/02/07 07:26:07 gshapiro Exp $  #####
#####  $Id: proto.m4,v 8.719 2006/03/30 20:50:13 ca Exp $  #####
# level 10 config file format
V10/Berkeley
# override file safeties - setting this option compromises system security,
# addressing the actual file configuration problem is preferred
# need to set this before any file actions are encountered in the cf file
#O DontBlameSendmail=safe
# default LDAP map specification
# need to set this now before any LDAP maps are defined
#O LDAPDefaultSpec=-h localhost
```

```
##################
#   local info   #
##################
# my LDAP cluster
# need to set this before any LDAP lookups are done (including classes)
#D{sendmailMTACluster}$m
Cwlocalhost
# file containing names of hosts for which we receive email
Fw/etc/mail/local-host-names
# my official domain name
# ... define this only if sendmail cannot automatically determine your domain
#Dj$w.Foo.COM
# host/domain names ending with a token in class P are canonical
CP.
# "Smart" relay host (may be null)
DS
# operators that cannot be in local usernames (i.e., network indicators)
CO @ % !
# a class with just dot (for identifying canonical names)
C..
# a class with just a left bracket (for identifying domain literals)
C[[
# access_db acceptance class
C{Accept}OK RELAY
C{ResOk}OKR
# Hosts for which relaying is permitted ($=R)
FR-o /etc/mail/relay-domains
# arithmetic map
```

Karith arith

macro storage map

Kmacro macro

possible values for TLS_connection in access map

C{Tls}VERIFY ENCR

dequoting map

Kdequote dequote

class E: names that should be exposed as from this host, even if we masquerade

class L: names that should be delivered locally, even if we have a relay

class M: domains that should be converted to $M

class N: domains that should not be converted to $M

#CL root

C{w}localhost.localdomain

CMlocalhost

CMrelais.bbs.fh-wilhelmshaven.de

CMlocalhost.localdomain

who I masquerade as (null for no masquerading) (see also $=M)

DMwebserver2012

my name for error messages

DnMAILER-DAEMON

Mailer table (overriding domains)

Kmailertable hash -o /etc/mail/mailertable.db

Virtual user table (maps incoming users)

Kvirtuser hash -o /etc/mail/virtusertable.db

CPREDIRECT

Access list database (for spam stomping)

Kaccess hash -T<TMPF> -o /etc/mail/access.db

Configuration version number

DZ8.13.8

```
###############
#   Options   #
###############
# strip message body to 7 bits on input?
O SevenBitInput=False
# 8-bit data handling
#O EightBitMode=pass8
# wait for alias file rebuild (default units: minutes)
O AliasWait=10
# location of alias file
O AliasFile=/etc/aliases
# minimum number of free blocks on filesystem
O MinFreeBlocks=100
# maximum message size
#O MaxMessageSize=0
# substitution for space (blank) characters
O BlankSub=.
# avoid connecting to "expensive" mailers on initial submission?
O HoldExpensive=False
# checkpoint queue runs after every N successful deliveries
#O CheckpointInterval=10
# default delivery mode
O DeliveryMode=background
# error message header/file
#O ErrorHeader=/etc/mail/error-header
# error mode
#O ErrorMode=print
```

```
# save Unix-style "From_" lines at top of header?
#O SaveFromLine=False
# queue file mode (qf files)
#O QueueFileMode=0600
# temporary file mode
O TempFileMode=0600
# match recipients against GECOS field?
#O MatchGECOS=False
# maximum hop count
#O MaxHopCount=25
# location of help file
O HelpFile=/etc/mail/helpfile
# ignore dots as terminators in incoming messages?
#O IgnoreDots=False
# name resolver options
#O ResolverOptions=+AAONLY
# deliver MIME-encapsulated error messages?
O SendMimeErrors=True
# Forward file search path
O ForwardPath=$z/.forward.$w:$z/.forward
# open connection cache size
O ConnectionCacheSize=2
# open connection cache timeout
O ConnectionCacheTimeout=5m
# persistent host status directory
#O HostStatusDirectory=.hoststat
# single thread deliveries (requires HostStatusDirectory)?
#O SingleThreadDelivery=False
```

use Errors-To: header?

O UseErrorsTo=False

log level

O LogLevel=9

send to me too, even in an alias expansion?

#O MeToo=True

verify RHS in newaliases?

O CheckAliases=False

default messages to old style headers if no special punctuation?

O OldStyleHeaders=True

SMTP daemon options

O DaemonPortOptions=Name=MTA,Port=smtp

SMTP client options

#O ClientPortOptions=Family=inet, Address=0.0.0.0

Modifiers to define {daemon_flags} for direct submissions

#O DirectSubmissionModifiers

Use as mail submission program? See sendmail/SECURITY

#O UseMSP

privacy flags

O PrivacyOptions=authwarnings,novrfy,noexpn,restrictqrun

who (if anyone) should get extra copies of error messages

#O PostmasterCopy=Postmaster

slope of queue-only function

#O QueueFactor=600000

limit on number of concurrent queue runners

#O MaxQueueChildren

maximum number of queue-runners per queue-grouping with multiple queues

#O MaxRunnersPerQueue=1

priority of queue runners (nice(3))

#O NiceQueueRun

shall we sort the queue by hostname first?

#O QueueSortOrder=priority

minimum time in queue before retry

#O MinQueueAge=30m

how many jobs can you process in the queue?

#O MaxQueueRunSize=0

perform initial split of envelope without checking MX records

#O FastSplit=1

queue directory

O QueueDirectory=/var/spool/mqueue

key for shared memory; 0 to turn off

#O SharedMemoryKey=0

timeouts (many of these)

#O Timeout.initial=5m

O Timeout.connect=1m

#O Timeout.aconnect=0s

#O Timeout.iconnect=5m

#O Timeout.helo=5m

#O Timeout.mail=10m

#O Timeout.rcpt=1h

#O Timeout.datainit=5m

#O Timeout.datablock=1h

#O Timeout.datafinal=1h

#O Timeout.rset=5m

#O Timeout.quit=2m

#O Timeout.misc=2m

#O Timeout.command=1h

O Timeout.ident=0

#O Timeout.fileopen=60s

#O Timeout.control=2m

O Timeout.queuereturn=5d

#O Timeout.queuereturn.normal=5d

#O Timeout.queuereturn.urgent=2d

#O Timeout.queuereturn.non-urgent=7d

#O Timeout.queuereturn.dsn=5d

O Timeout.queuewarn=4h

#O Timeout.queuewarn.normal=4h

#O Timeout.queuewarn.urgent=1h

#O Timeout.queuewarn.non-urgent=12h

#O Timeout.queuewarn.dsn=4h

#O Timeout.hoststatus=30m

#O Timeout.resolver.retrans=5s

#O Timeout.resolver.retrans.first=5s

#O Timeout.resolver.retrans.normal=5s

#O Timeout.resolver.retry=4

#O Timeout.resolver.retry.first=4

#O Timeout.resolver.retry.normal=4

#O Timeout.lhlo=2m

#O Timeout.auth=10m

#O Timeout.starttls=1h

time for DeliverBy; extension disabled if less than 0

#O DeliverByMin=0

should we not prune routes in route-addr syntax addresses?

#O DontPruneRoutes=False

```
# queue up everything before forking?
O SuperSafe=True
# status file
O StatusFile=/var/log/mail/statistics
# time zone handling:
#  if undefined, use system default
#  if defined but null, use TZ envariable passed in
#  if defined and non-null, use that info
#O TimeZoneSpec=
# default UID (can be username or userid:groupid)
O DefaultUser=8:12
# list of locations of user database file (null means no lookup)
O UserDatabaseSpec=/etc/mail/userdb.db
# fallback MX host
#O FallbackMXhost=fall.back.host.net
# fallback smart host
#O FallbackSmartHost=fall.back.host.net
# if we are the best MX host for a site, try it directly instead of config err
O TryNullMXList=True
# load average at which we just queue messages
#O QueueLA=8
# load average at which we refuse connections
#O RefuseLA=12
# log interval when refusing connections for this long
#O RejectLogInterval=3h
# load average at which we delay connections; 0 means no limit
#O DelayLA=0
# maximum number of children we allow at one time
```

#O MaxDaemonChildren=0

maximum number of new connections per second

#O ConnectionRateThrottle=0

Width of the window

#O ConnectionRateWindowSize=60s

work recipient factor

#O RecipientFactor=30000

deliver each queued job in a separate process?

#O ForkEachJob=False

work class factor

#O ClassFactor=1800

work time factor

#O RetryFactor=90000

default character set

#O DefaultCharSet=unknown-8bit

service switch file (name hardwired on Solaris, Ultrix, OSF/1, others)

#O ServiceSwitchFile=/etc/mail/service.switch

hosts file (normally /etc/hosts)

#O HostsFile=/etc/hosts

dialup line delay on connection failure

#O DialDelay=0s

action to take if there are no recipients in the message

#O NoRecipientAction=none

chrooted environment for writing to files

#O SafeFileEnvironment

are colons OK in addresses?

#O ColonOkInAddr=True

shall I avoid expanding CNAMEs (violates protocols)?

```
#O DontExpandCnames=False

# SMTP initial login message (old $e macro)

O SmtpGreetingMessage=$j Sendmail $v/$Z; $b

# UNIX initial From header format (old $l macro)

O UnixFromLine=From $g $d

# From: lines that have embedded newlines are unwrapped onto one line

#O SingleLineFromHeader=False

# Allow HELO SMTP command that does not include a host name

#O AllowBogusHELO=False

# Characters to be quoted in a full name phrase (@,;:\()[] are automatic)

#O MustQuoteChars=.

# delimiter (operator) characters (old $o macro)

O OperatorChars=.:%@!^/[]+

# shall I avoid calling initgroups(3) because of high NIS costs?

#O DontInitGroups=False

# are group-writable :include: and .forward files (un)trustworthy?

# True (the default) means they are not trustworthy.

#O UnsafeGroupWrites=True

# where do errors that occur when sending errors get sent?

#O DoubleBounceAddress=postmaster

# where to save bounces if all else fails

#O DeadLetterDrop=/var/tmp/dead.letter

# what user id do we assume for the majority of the processing?

#O RunAsUser=sendmail

# maximum number of recipients per SMTP envelope

#O MaxRecipientsPerMessage=0

# limit the rate recipients per SMTP envelope are accepted

# once the threshold number of recipients have been rejected
```

```
#O BadRcptThrottle=0

# shall we get local names from our installed interfaces?

O DontProbeInterfaces=True

# Return-Receipt-To: header implies DSN request

#O RrtImpliesDsn=False

# override connection address (for testing)

#O ConnectOnlyTo=0.0.0.0

# Trusted user for file ownership and starting the daemon

#O TrustedUser=root

# Control socket for daemon management

#O ControlSocketName=/var/spool/mqueue/.control

# Maximum MIME header length to protect MUAs

#O MaxMimeHeaderLength=0/0

# Maximum length of the sum of all headers

#O MaxHeadersLength=32768

# Maximum depth of alias recursion

#O MaxAliasRecursion=10

# location of pid file

#O PidFile=/var/run/sendmail.pid

# Prefix string for the process title shown on 'ps' listings

#O ProcessTitlePrefix=prefix

# Data file (df) memory-buffer file maximum size

#O DataFileBufferSize=4096

# Transcript file (xf) memory-buffer file maximum size

#O XscriptFileBufferSize=4096

# lookup type to find information about local mailboxes

#O MailboxDatabase=pw

# override compile time flag REQUIRES_DIR_FSYNC
```

#O RequiresDirfsync=true

list of authentication mechanisms

#O AuthMechanisms=EXTERNAL GSSAPI KERBEROS_V4 DIGEST-MD5 CRAM-MD5

Authentication realm

#O AuthRealm

default authentication information for outgoing connections

#O DefaultAuthInfo=/etc/mail/default-auth-info

SMTP AUTH flags

O AuthOptions=A

SMTP AUTH maximum encryption strength

#O AuthMaxBits

SMTP STARTTLS server options

#O TLSSrvOptions

Input mail filters

O InputMailFilters=avmilter

Milter options

#O Milter.LogLevel

O Milter.macros.connect=j, _, {daemon_name}, {if_name}, {if_addr}

O Milter.macros.helo={tls_version}, {cipher}, {cipher_bits}, {cert_subject}, {cert_issuer}

O Milter.macros.envfrom=i, {auth_type}, {auth_authen}, {auth_ssf}, {auth_author}, {mail_mailer}, {mail_host}, {mail_addr}

O Milter.macros.envrcpt={rcpt_mailer}, {rcpt_host}, {rcpt_addr}

O Milter.macros.eom={msg_id}

CA directory

#O CACertPath

CA file

#O CACertFile

Server Cert

#O ServerCertFile

Server private key

#O ServerKeyFile

Client Cert

#O ClientCertFile

Client private key

#O ClientKeyFile

File containing certificate revocation lists

#O CRLFile

DHParameters (only required if DSA/DH is used)

#O DHParameters

Random data source (required for systems without /dev/urandom under OpenSSL)

#O RandFile

############################

QUEUE GROUP DEFINITIONS

############################

############################

Message precedences

############################

Pfirst-class=0

Pspecial-delivery=100

Plist=-30

Pbulk=-60

Pjunk=-100

####################

Trusted users

####################

this is equivalent to setting class "t"

Ft/etc/mail/trusted-users

Troot

Tdaemon

Tuucp

########################

Format of headers

########################

H?P?Return-Path: <$g>

HReceived: $?sfrom $s $.$?_($?s$|from $.$_)

$.$?{auth_type}(authenticated$?{auth_ssf} bits=${auth_ssf}$.)

$.by $j ($v/$Z)$?r with r. id i?{tls_version}

(version=${tls_version} cipher=${cipher} bits=${cipher_bits} verify=${verify})$.$?u

for $u; $|;

$.$b

H?D?Resent-Date: $a

H?D?Date: $a

H?F?Resent-From: $?x$x <$g>$|g.

H?F?From: $?x$x <$g>$|g.

H?x?Full-Name: $x

HPosted-Date: $a

H?l?Received-Date: $b

H?M?Resent-Message-Id: <$t.$i@$j>

H?M?Message-Id: <$t.$i@$j>

#

```
######################################################################
######################################################################
#####
#####                    REWRITING RULES
#####
######################################################################
######################################################################
##############################################
###  Ruleset 3 -- Name Canonicalization  ###
##############################################
Scanonify=3
# handle null input (translate to <@> special case)
R$@                     $@ <@>
# strip group: syntax (not inside angle brackets!) and trailing semicolon
R$*                     $: $1 <@>                       mark addresses
R$* < $* > $* <@>       $: $1 < $2 > $3                 unmark <addr>
R@ $* <@>               $: @ $1                         unmark @host:...
R$* [ IPv6 : $+ ] <@>   $: $1 [ IPv6 : $2 ]             unmark IPv6 addr
R$* :: $* <@>           $: $1 :: $2                     unmark node::addr
R:include: $* <@>       $: :include: $1                 unmark :include:...
R$* : $* [ $* ]         $: $1 : $2 [ $3 ] <@>           remark if leading colon
R$* : $* <@>            $: $2                           strip colon if marked
R$* <@>                         $: $1                           unmark
R$* ;                     $1                            strip trailing semi
R$* < $+ :; > $*        $@ $2 :; <@>                    catch <list:;>
R$* < $* ; >              $1 < $2 >                     bogus bracketed semi
# null input now results from list:; syntax
R$@                     $@ :; <@>
```

```
# strip angle brackets -- note RFC733 heuristic to get innermost item
R$*                     $: < $1 >                       housekeeping <>
R$+ < $* >              < $2 >                          strip excess on left
R< $* > $+              < $1 >                          strip excess on right
R<>                     $@ < @ >                        MAIL FROM:<> case
R< $+ >                         $: $1                           remove housekeeping <>
# strip route address <@a,@b,@c:user@d> -> <user@d>
R@ $+ , $+              $2
R@ [ $* ] : $+          $2
R@ $+ : $+              $2
# find focus for list syntax
R $+ : $* ; @ $+        $@ $>Canonify2 $1 : $2 ; < @ $3 >       list syntax
R $+ : $* ;             $@ $1 : $2;                     list syntax
# find focus for @ syntax addresses
R$+ @ $+                $: $1 < @ $2 >                  focus on domain
R$+ < $+ @ $+ >                 $1 $2 < @ $3 >                  move gaze right
R$+ < @ $+ >            $@ $>Canonify2 $1 < @ $2 >      already canonical
# convert old-style addresses to a domain-based address
R$- ! $+                $@ $>Canonify2 $2 < @ $1 .UUCP >        resolve uucp names
R$+ . $- ! $+           $@ $>Canonify2 $3 < @ $1 . $2 >                 domain uucps
R$+ ! $+                $@ $>Canonify2 $2 < @ $1 .UUCP >        uucp subdomains
# if we have % signs, take the rightmost one
R$* % $*                $1 @ $2                         First make them all @s.
R$* @ $* @ $*                   $1 % $2 @ $3                    Undo all but the last.
R$* @ $*                $@ $>Canonify2 $1 < @ $2 >      Insert < > and finish
# else we must be a local name
R$*                     $@ $>Canonify2 $1
```

```
################################################
###  Ruleset 96 -- bottom half of ruleset 3  ###
################################################
SCanonify2=96
# handle special cases for local names
R$* < @ localhost > $*          $: $1 < @ $j . > $2             no domain at all
R$* < @ localhost . $m > $*     $: $1 < @ $j . > $2             local domain
R$* < @ localhost . UUCP > $*           $: $1 < @ $j . > $2             .UUCP domain
# check for IPv4/IPv6 domain literal
R$* < @ [ $+ ] > $*             $: $1 < @@ [ $2 ] > $3          mark [addr]
R$* < @@ $=w > $*               $: $1 < @ $j . > $3             self-literal
R$* < @@ $+ > $*                $@ $1 < @ $2 > $3               canon IP addr
# if really UUCP, handle it immediately
# try UUCP traffic as a local address
R$* < @ $+ . UUCP > $*                  $: $1 < @ $[ $2 $] . UUCP . > $3
R$* < @ $+ . . UUCP . > $*      $@ $1 < @ $2 . > $3
# hostnames ending in class P are always canonical
R$* < @ $* $=P > $*             $: $1 < @ $2 $3 . > $4
R$* < @ $* $~P > $*             $: $&{daemon_flags} $| $1 < @ $2 $3 > $4
R$* CC $* $| $* < @ $+.$+ > $*          $: $3 < @ $4.$5 . > $6
R$* CC $* $| $*                         $: $3
# pass to name server to make hostname canonical
R$* $| $* < @ $* > $*           $: $2 < @ $[ $3 $] > $4
R$* $| $*                       $: $2
# local host aliases and pseudo-domains are always canonical
R$* < @ $=w > $*                $: $1 < @ $2 . > $3
R$* < @ $=M > $*                $: $1 < @ $2 . > $3
R$* < @ $={VirtHost} > $*       $: $1 < @ $2 . > $3
```

```
R$* < @ $* . . > $*              $1 < @ $2 . > $3
##################################################
###  Ruleset 4 -- Final Output Post-rewriting  ###
##################################################
Sfinal=4
R$+ :; <@>              $@ $1 :                  handle <list:;>
R$* <@>                 $@                       handle <> and list:;
# strip trailing dot off possibly canonical name
R$* < @ $+ . > $*       $1 < @ $2 > $3
# eliminate internal code
R$* < @ *LOCAL* > $*    $1 < @ $j > $2
# externalize local domain info
R$* < $+ > $*           $1 $2 $3                 defocus
R@ $+ : @ $+ : $+       @ $1 , @ $2 : $3         <route-addr> canonical
R@ $*                   $@ @ $1                  ... and exit
# UUCP must always be presented in old form
R$+ @ $- . UUCP         $2!$1                    u@h.UUCP => h!u
# delete duplicate local names
R$+ % $=w @ $=w         $1 @ $2                  u%host@host => u@host
##################################################################
###   Ruleset 97 -- recanonicalize and call ruleset zero   ###
###                (used for recursive calls)                  ###
##################################################################
SRecurse=97
R$*                     $: $>canonify $1
R$*                     $@ $>parse $1
```

```
######################################
###   Ruleset 0 -- Parse Address   ###
######################################
Sparse=0
R$*                     $: $>Parse0 $1          initial parsing
R<@>                    $#local $: <@>          special case error msgs
R$*                     $: $>ParseLocal $1      handle local hacks
R$*                     $: $>Parse1 $1          final parsing
#
#  Parse0 -- do initial syntax checking and eliminate local addresses.
#         This should either return with the (possibly modified) input
#         or return with a #error mailer.  It should not return with a
#         #mailer other than the #error mailer.
#
SParse0
R<@>                    $@ <@>                          special case error msgs
R$* : $* ; <@>          $#error $@ 5.1.3 $: "553 List:; syntax illegal for recipient addresses"
R@ <@ $* >              < @ $1 >                catch "@@host" bogosity
R<@ $+>                         $#error $@ 5.1.3 $: "553 User address required"
R$+ <@>                         $#error $@ 5.1.3 $: "553 Hostname required"
R$*                     $: <> $1
R<> $* < @ [ $* ] : $+ > $*     $1 < @ [ $2 ] : $3 > $4
R<> $* < @ [ $* ] , $+ > $*     $1 < @ [ $2 ] , $3 > $4
R<> $* < @ [ $* ] $+ > $*       $#error $@ 5.1.2 $: "553 Invalid address"
R<> $* < @ [ $+ ] > $*          $1 < @ [ $2 ] > $3
R<> $* <$* : $* > $*    $#error $@ 5.1.3 $: "553 Colon illegal in host name part"
R<> $*                  $1
R$* < @ . $* > $*       $#error $@ 5.1.2 $: "553 Invalid host name"
```

```
R$* < @ $* .. $* > $*   $#error $@ 5.1.2 $: "553 Invalid host name"
R$* < @ $* @ > $*       $#error $@ 5.1.2 $: "553 Invalid route address"
R$* @ $* < @ $* > $*    $#error $@ 5.1.3 $: "553 Invalid route address"
R$* , $~O $*            $#error $@ 5.1.3 $: "553 Invalid route address"
# now delete the local info -- note $=O to find characters that cause forwarding
R$* < @ > $*            $@ $>Parse0 $>canonify $1       user@ => user
R< @ $=w . > : $*       $@ $>Parse0 $>canonify $2       @here:... -> ...
R$- < @ $=w . >                 $: $(dequote $1 $) < @ $2 . >   dequote "foo"@here
R< @ $+ >               $#error $@ 5.1.3 $: "553 User address required"
R$* $=O $* < @ $=w . >          $@ $>Parse0 $>canonify $1 $2 $3         ...@here -> ...
R$-                     $: $(dequote $1 $) < @ *LOCAL* >        dequote "foo"
R< @ *LOCAL* >                  $#error $@ 5.1.3 $: "553 User address required"
R$* $=O $* < @ *LOCAL* >
                        $@ $>Parse0 $>canonify $1 $2 $3         ...@*LOCAL* -> ...
R$* < @ *LOCAL* >       $: $1
#
#  Parse1 -- the bottom half of ruleset 0.
#
SParse1
# handle numeric address spec
R$* < @ [ $+ ] > $*     $: $>ParseLocal $1 < @ [ $2 ] > $3      numeric internet spec
R$* < @ [ $+ ] > $*     $: $1 < @ [ $2 ] : $S > $3      Add smart host to path
R$* < @ [ $+ ] : > $*           $#esmtp $@ [$2] $: $1 < @ [$2] > $3     no smarthost: send
R$* < @ [ $+ ] : $- : $*> $*    $#$3 $@ $4 $: $1 < @ [$2] > $5          smarthost with mailer
R$* < @ [ $+ ] : $+ > $*        $#esmtp $@ $3 $: $1 < @ [$2] > $4       smarthost without mailer
# handle virtual users
R$+                     $: <!> $1               Mark for lookup
R<!> $+ < @ $={VirtHost} . > $: < $(virtuser $1 @ $2 $@ $1 $: @ $) > $1 < @ $2 . >
```

R<!> $+ < @ $=w . > $: < $(virtuser $1 @ $2 $@ $1 $: @ $) > $1 < @ $2 . >

R<@> $+ + $+ < @ $* . >

$: < $(virtuser $1 + + @ $3 $@ $1 $@ $2 $@ +$2 $: @ $) > $1 + $2 < @ $3 . >

R<@> $+ + $* < @ $* . >

$: < $(virtuser $1 + * @ $3 $@ $1 $@ $2 $@ +$2 $: @ $) > $1 + $2 < @ $3 . >

R<@> $+ + $* < @ $* . >

$: < $(virtuser $1 @ $3 $@ $1 $@ $2 $@ +$2 $: @ $) > $1 + $2 < @ $3 . >

R<@> $+ + $+ < @ $+ . > $: < $(virtuser + + @ $3 $@ $1 $@ $2 $@ +$2 $: @ $) > $1 + $2 < @ $3 . >

R<@> $+ + $* < @ $+ . > $: < $(virtuser + * @ $3 $@ $1 $@ $2 $@ +$2 $: @ $) > $1 + $2 < @ $3 . >

R<@> $+ + $* < @ $+ . > $: < $(virtuser @ $3 $@ $1 $@ $2 $@ +$2 $: ! $) > $1 + $2 < @ $3 . >

R<@> $+ < @ $+ . > $: < $(virtuser @ $2 $@ $1 $: @ $) > $1 < @ $2 . >

R<@> $+ $: $1

R<!> $+ $: $1

R< error : $-.$-.$- : $+ > $* $#error $@ $1.$2.$3 $: $4

R< error : $- $+ > $* $#error $@ $(dequote $1 $) $: $2

R< $+ > $+ < @ $+ > $: $>Recurse $1

short circuit local delivery so forwarded email works

R$=L < @ $=w . > $#local $: @ $1 special local names

R$+ < @ $=w . > $#local $: $1 regular local name

not local -- try mailer table lookup

R$* <@ $+ > $* $: < $2 > $1 < @ $2 > $3 extract host name

R< $+ . > $* $: < $1 > $2 strip trailing dot

R< $+ > $* $: < $(mailertable $1 $) > $2 lookup

R< $~[: $* > $* $>MailerToTriple < $1 : $2 > $3 check -- resolved?

R< $+ > $* $: $>Mailertable <$1> $2 try domain

```
# resolve remotely connected UUCP links (if any)

# resolve fake top level domains by forwarding to other hosts

# pass names that still have a host to a smarthost (if defined)

R$* < @ $* > $*                 $: $>MailerToTriple < $S > $1 < @ $2 > $3      glue on smarthost
name

# deal with other remote names

R$* < @$* > $*                  $#esmtp $@ $2 $: $1 < @ $2 > $3        user@host.domain

# handle locally delivered names

R$=L                    $#local $: @ $1          special local names

R$+                     $#local $: $1                    regular local names

##########################################################################

###   Ruleset 5 -- special rewriting after aliases have been expanded   ###

##########################################################################

SLocal_localaddr

Slocaladdr=5

R$+                     $: $1 $| $>"Local_localaddr" $1

R$+ $| $#ok             $@ $1                    no change

R$+ $| $#$*             $#$2

R$+ $| $*               $: $1

# deal with plussed users so aliases work nicely

R$+ + *                         $#local $@ $&h $: $1

R$+ + $*                $#local $@ + $2 $: $1 + *

# prepend an empty "forward host" on the front

R$+                     $: <> $1

R< > $+                         $: < > < $1 <> $&h >             nope, restore +detail

R< > < $+ <> + $* >     $: < > < $1 + $2 >               check whether +detail

R< > < $+ <> $* >       $: < > < $1 >                    else discard

R< > < $+ + $* > $*       < > < $1 > + $2 $3             find the user part
```

```
R< > < $+ > + $*        $#local $@ $2 $: @ $1          strip the extra +
R< > < $+ >             $@ $1                          no +detail
R$+                     $: $1 <> $&h                   add +detail back in
R$+ <> + $*             $: $1 + $2                     check whether +detail
R$+ <> $*               $: $1                          else discard
R< local : $* > $*      $: $>MailerToTriple < local : $1 > $2    no host extension
R< error : $* > $*      $: $>MailerToTriple < error : $1 > $2    no host extension
R< $~[ : $+ > $+        $: $>MailerToTriple < $1 : $2 > $3 < @ $2 >
R< $+ > $+              $@ $>MailerToTriple < $1 > $2 < @ $1 >
##########################################################################
###  Ruleset 90 -- try domain part of mailertable entry   ###
##########################################################################
SMailertable=90
R$* <$- . $+ > $*       $: $1$2 < $(mailertable .$3 $@ $1$2 $@ $2 $) > $4
R$* <$~[ : $* > $*      $>MailerToTriple < $2 : $3 > $4                  check -- resolved?
R$* < . $+ > $*         $@ $>Mailertable $1 . <$2> $3          no -- strip & try again
R$* < $* > $*           $: < $(mailertable . $@ $1$2 $) > $3   try "."
R< $~[ : $* > $*        $>MailerToTriple < $1 : $2 > $3                  "." found?
R< $* > $*              $@ $2                          no mailertable match
##########################################################################
###  Ruleset 95 -- canonify mailer:[user@]host syntax to triple  ###
##########################################################################
SMailerToTriple=95
R< > $*                         $@ $1                  strip off null relay
R< error : $-.$-.$- : $+ > $*   $#error $@ $1.$2.$3 $: $4
R< error : $- : $+ > $*         $#error $@ $(dequote $1 $) $: $2
R< error : $+ > $*              $#error $: $1
R< local : $* > $*              $>CanonLocal < $1 > $2
```

```
R< $~[ : $+ @ $+ > $*<$*>$*  $# $1 $@ $3 $: $2<@$3>        use literal user
R< $~[ : $+ > $*             $# $1 $@ $2 $: $3       try qualified mailer
R< $=w > $*                  $@ $2                   delete local host
R< $+ > $*                   $#relay $@ $1 $: $2     use unqualified mailer
######################################################################
###  Ruleset CanonLocal -- canonify local: syntax                  ###
######################################################################
SCanonLocal
# strip local host from routed addresses
R< $* > < @ $+ > : $+        $@ $>Recurse $3
R< $* > $+ $=O $+ < @ $+ >   $@ $>Recurse $2 $3 $4
# strip trailing dot from any host name that may appear
R< $* > $* < @ $* . >        $: < $1 > $2 < @ $3 >
# handle local: syntax -- use old user, either with or without host
R< > $* < @ $* > $*          $#local $@ $1@$2 $: $1
R< > $+                              $#local $@ $1    $: $1
# handle local:user@host syntax -- ignore host part
R< $+ @ $+ > $* < @ $* >     $: < $1 > $3 < @ $4 >
# handle local:user syntax
R< $+ > $* <@ $* > $*                $#local $@ $2@$3 $: $1
R< $+ > $*                   $#local $@ $2    $: $1
######################################################################
###  Ruleset 93 -- convert header names to masqueraded form    ###
######################################################################
SMasqHdr=93
# do not masquerade anything in class N
R$* < @ $* $=N . >     $@ $1 < @ $2 $3 . >
# special case the users that should be exposed
```

R$=E < @ *LOCAL* > $@ $1 < @ $j . > leave exposed

R$=E < @ $=M . > $@ $1 < @ $2 . >

R$=E < @ $=w . > $@ $1 < @ $2 . >

handle domain-specific masquerading

R$* < @ $=M . > $* $: $1 < @ $2 . @ $M > $3 convert masqueraded doms

R$* < @ $=w . > $* $: $1 < @ $2 . @ $M > $3

R$* < @ *LOCAL* > $* $: $1 < @ $j . @ $M > $2

R$* < @ $+ @ > $* $: $1 < @ $2 > $3 $M is null

R$* < @ $+ @ $+ > $* $: $1 < @ $3 . > $4 $M is not null

##

Ruleset 94 -- convert envelope names to masqueraded form

##

SMasqEnv=94

R$* < @ *LOCAL* > $* $: $1 < @ $j . > $2

##

Ruleset 98 -- local part of ruleset zero (can be null)###

##

SParseLocal=98

addresses sent to foo@host.REDIRECT will give a 551 error code

R$* < @ $+ .REDIRECT. > $: $1 < @ $2 . REDIRECT . > < ${opMode} >

R$* < @ $+ .REDIRECT. > <i> $: $1 < @ $2 . REDIRECT. >

R$* < @ $+ .REDIRECT. > < $- > $#error $@ 5.1.1 $: "551 User has moved; please try "
<$1@$2>

##

D: LookUpDomain -- search for domain in access database

###

Parameters:

<$1> -- key (domain name)

```
###             <$2> -- default (what to return if not found in db)
###             <$3> -- mark (must be <(!|+) single-token>)
###                     ! does lookup only with tag
###                     + does lookup with and without tag
###             <$4> -- passthru (additional data passed unchanged through)
#########################################################################
SD
R<$*> <$+> <$- $-> <$*>                 $: < $(access $4:$1 $: ? $) > <$1> <$2> <$3 $4> <$5>
R<?> <$+> <$+> <+ $-> <$*> $: < $(access $1 $: ? $) > <$1> <$2> <+ $3> <$4>
R<?> <[$+.$-]> <$+> <$- $-> <$*>    $@ $>D <[$1]> <$3> <$4 $5> <$6>
R<?> <[$+::$-]> <$+> <$- $-> <$*>   $: $>D <[$1]> <$3> <$4 $5> <$6>
R<?> <[$+:$-]> <$+> <$- $-> <$*>    $: $>D <[$1]> <$3> <$4 $5> <$6>
R<?> <$+.$+> <$+> <$- $-> <$*>      $@ $>D <$2> <$3> <$4 $5> <$6>
R<?> <$+> <$+> <$- $-> <$*>$@ <$2> <$5>
R<$* <TMPF>> <$+> <$+> <$- $-> <$*>     $@ <<TMPF>> <$6>
R<$*> <$+> <$+> <$- $-> <$*>        $@ <$1> <$6>
#########################################################################
###  A: LookUpAddress -- search for host address in access database
###
###     Parameters:
###             <$1> -- key (dot quadded host address)
###             <$2> -- default (what to return if not found in db)
###             <$3> -- mark (must be <(!|+) single-token>)
###                     ! does lookup only with tag
###                     + does lookup with and without tag
###             <$4> -- passthru (additional data passed through)
```

```
##########################################################################
SA
R<$+> <$+> <$- $-> <$*>                 $: < $(access $4:$1 $: ? $) > <$1> <$2> <$3 $4> <$5>
R<?> <$+> <$+> <+ $-> <$*> $: < $(access $1 $: ? $) > <$1> <$2> <+ $3> <$4>
R<?> <$+::$-> <$+> <$- $-> <$*>                 $@ $>A <$1> <$3> <$4 $5> <$6>
R<?> <$+:$-> <$+> <$- $-> <$*>                  $@ $>A <$1> <$3> <$4 $5> <$6>
R<?> <$+.$-> <$+> <$- $-> <$*>                  $@ $>A <$1> <$3> <$4 $5> <$6>
R<?> <$+> <$+> <$- $-> <$*>$@ <$2> <$5>
R<$* <TMPF>> <$+> <$+> <$- $-> <$*>     $@ <<TMPF>> <$6>
R<$*> <$+> <$+> <$- $-> <$*>            $@ <$1> <$6>
##########################################################################
###  CanonAddr --       Convert an address into a standard form for
###                     relay checking.  Route address syntax is
###                     crudely converted into a %-hack address.
###
###      Parameters:
###              $1 -- full recipient address
###
###      Returns:
###              parsed address, not in source route form
##########################################################################
SCanonAddr
R$*                     $: $>Parse0 $>canonify $1       make domain canonical
##########################################################################
###  ParseRecipient --  Strip off hosts in $=R as well as possibly
###                     $* $=m or the access database.
###                     Check user portion for host separators.
```

```
###
###     Parameters:
###             $1 -- full recipient address
###
###     Returns:
###             parsed, non-local-relaying address
##########################################################################
SParseRecipient
R$*                     $: <?> $>CanonAddr $1
R<?> $* < @ $* . >      <?> $1 < @ $2 >                 strip trailing dots
R<?> $- < @ $* >        $: <?> $(dequote $1 $) < @ $2 >     dequote local part
# if no $=O character, no host in the user portion, we are done
R<?> $* $=O $* < @ $* >         $: <NO> $1 $2 $3 < @ $4>
R<?> $*                         $@ $1
R<NO> $* < @ $* $=R >           $: <RELAY> $1 < @ $2 $3 >
R<NO> $* < @ $+ >       $: $>D <$2> <NO> <+ To> <$1 < @ $2 >>
R<$+> <$+>              $: <$1> $2
R<RELAY> $* < @ $* >            $@ $>ParseRecipient $1
R<$+> $*                $@ $2
##########################################################################
###  check_relay -- check hostname/address on SMTP startup
##########################################################################
SLocal_check_relay
Scheck_relay
R$*                     $: $1 $| $>"Local_check_relay" $1
R$* $| $* $| $#$*       $#$3
R$* $| $* $| $*         $@ $>"Basic_check_relay" $1 $| $2
SBasic_check_relay
```

```
# check for deferred delivery mode
R$*                     $: < $&{deliveryMode} > $1
R< d > $*               $@ deferred
R< $* > $*              $: $2
R$+ $| $+               $: $>D < $1 > <?> <+ Connect> < $2 >
R   $| $+               $: $>A < $1 > <?> <+ Connect> <>      empty client_name
R<?> <$+>               $: $>A < $1 > <?> <+ Connect> <>      no: another lookup
R<?> <$*>               $: OK                                 found nothing
R<$={Accept}> <$*>      $@ $1                                 return value of lookup
R<REJECT> <$*>          $#error $@ 5.7.1 $: "550 Access denied"
R<DISCARD> <$*>         $#discard $: discard
R<QUARANTINE:$+> <$*>   $#error $@ quarantine $: $1
R<ERROR:$-.$-.$-:$+> <$*>  $#error $@ $1.$2.$3 $: $4
R<ERROR:$+> <$*>        $#error $: $1
R<$* <TMPF>> <$*>       $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again
later."
R<$+> <$*>              $#error $: $1
##########################################################################
###  check_mail -- check SMTP `MAIL FROM:' command argument
##########################################################################
SLocal_check_mail
Scheck_mail
R$*                     $: $1 $| $>"Local_check_mail" $1
R$* $| $#$*             $#$2
R$* $| $*               $@ $>"Basic_check_mail" $1
SBasic_check_mail
# check for deferred delivery mode
R$*                     $: < $&{deliveryMode} > $1
```

```
R< d > $*               $@ deferred
R< $* > $*              $: $2
# authenticated?
R$*                     $: $1 $| $>"tls_client" $&{verify} $| MAIL
R$* $| $#$+             $#$2
R$* $| $*               $: $1
R<>                     $@ <OK>                 we MUST accept <> (RFC 1123)
R$+                     $: <?> $1
R<?><$+>                $: <@> <$1>
R<?>$+                  $: <@> <$1>
R$*                     $: $&{daemon_flags} $| $1
R$* f $* $| <@> < $* @ $- >     $: < ? $&{client_name} > < $3 @ $4 >
R$* u $* $| <@> < $* >          $: <?> < $3 >
R$* $| $*               $: $2
# handle case of @localhost on address
R<@> < $* @ localhost >         $: < ? $&{client_name} > < $1 @ localhost >
R<@> < $* @ [127.0.0.1] >
                        $: < ? $&{client_name} > < $1 @ [127.0.0.1] >
R<@> < $* @ localhost.$m >
                        $: < ? $&{client_name} > < $1 @ localhost.$m >
R<@> < $* @ localhost.localdomain >
                        $: < ? $&{client_name} > < $1 @ localhost.localdomain >
R<@> < $* @ localhost.UUCP >
                        $: < ? $&{client_name} > < $1 @ localhost.UUCP >
R<@> $*                 $: $1                   no localhost as domain
R<? $=w> $*             $: $2                   local client: ok
R<? $+> <$+>            $#error $@ 5.5.4 $: "553 Real domain name required for sender address"
R<?> $*                 $: $1
```

```
R$*                     $: <?> $>CanonAddr $1                   canonify sender address and mark it
R<?> $* < @ $+ . >      <?> $1 < @ $2 >                         strip trailing dots
# handle non-DNS hostnames (*.bitnet, *.decnet, *.uucp, etc)
R<?> $* < @ $* $=P >    $: <OKR> $1 < @ $2 $3 >
R<?> $* < @ $j >        $: <OKR> $1 < @ $j >
R<?> $* < @ $+ >        $: <OKR> $1 < @ $2 >            ... unresolvable OK
# check sender address: user@address, user@, address
R<$+> $+ < @ $* >       $: @<$1> <$2 < @ $3 >> $| <F:$2@$3> <U:$2@> <D:$3>
R<$+> $+                $: @<$1> <$2> $| <U:$2@>
R@ <$+> <$*> $| <$+>            $: <@> <$1> <$2> $| $>SearchList <+ From> $| <$3> <>
R<@> <$+> <$*> $| <$*>          $: <$3> <$1> <$2>               reverse result
# retransform for further use
R<?> <$+> <$*>                  $: <$1> $2      no match
R<$+> <$+> <$*>                 $: <$1> $3      relevant result, keep it
# handle case of no @domain on address
R<?> $*                         $: $&{daemon_flags} $| <?> $1
R$* u $* $| <?> $*      $: <OKR> $3
R$* $| $*               $: $2
R<?> $*                         $: < ? $&{client_addr} > $1
R<?> $*                         $@ <OKR>                        ...local unqualed ok
R<? $+> $*              $#error $@ 5.5.4 $: "553 Domain name required for sender address " $&f
                                                                ...remote is not
# check results
R<?> $*                         $: @ $1         mark address: nothing known about it
R<$={ResOk}> $*                 $@ <OKR>        domain ok: stop
R<TEMP> $*              $#error $@ 4.1.8 $: "451 Domain of sender address " $&f " does not resolve"
R<PERM> $*              $#error $@ 5.1.8 $: "553 Domain of sender address " $&f " does not exist"
R<$={Accept}> $*        $# $1           accept from access map
```

```
R<DISCARD> $*                   $#discard $: discard
R<QUARANTINE:$+> $*             $#error $@ quarantine $: $1
R<REJECT> $*                    $#error $@ 5.7.1 $: "550 Access denied"
R<ERROR:$-.$-.$-:$+> $*                 $#error $@ $1.$2.$3 $: $4
R<ERROR:$+> $*                  $#error $: $1
R<<TMPF>> $*                    $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again
later."
R<$+> $*                $#error $: $1               error from access db
##########################################################################
###  check_rcpt -- check SMTP `RCPT TO:' command argument
##########################################################################
SLocal_check_rcpt
Scheck_rcpt
R$*                     $: $1 $| $>"Local_check_rcpt" $1
R$* $| $#$*             $#$2
R$* $| $*               $@ $>"Basic_check_rcpt" $1
SBasic_check_rcpt
# empty address?
R<>                     $#error $@ nouser $: "553 User address required"
R$@                     $#error $@ nouser $: "553 User address required"
# check for deferred delivery mode
R$*                     $: < $&{deliveryMode} > $1
R< d > $*               $@ deferred
R< $* > $*              $: $2
```

```
##########################################################################
R$*                     $: $1 $| @ $>"Rcpt_ok" $1
R$* $| @ $#TEMP $+      $: $1 $| T $2
R$* $| @ $#$*           $#$2
R$* $| @ RELAY                  $@ RELAY
R$* $| @ $*             $: O $| $>"Relay_ok" $1
R$* $| T $+             $: T $2 $| $>"Relay_ok" $1
R$* $| $#TEMP $+        $#error $2
R$* $| $#$*             $#$2
R$* $| RELAY            $@ RELAY
R T $+ $| $*            $#error $1
# anything else is bogus
R$*                     $#error $@ 5.7.1 $: "550 Relaying denied"
##########################################################################
### Rcpt_ok: is the recipient ok?
##########################################################################
SRcpt_ok
R$*                     $: $>ParseRecipient $1          strip relayable hosts
# blacklist local users or any host from receiving mail
R$*                     $: <?> $1
R<?> $+ < @ $=w >       $: <> <$1 < @ $2 >> $| <F:$1@$2> <U:$1@> <D:$2>
R<?> $+ < @ $* >        $: <> <$1 < @ $2 >> $| <F:$1@$2> <D:$2>
R<?> $+                         $: <> <$1> $| <U:$1@>
R<> <$*> $| <$+>        $: <@> <$1> $| $>SearchList <+ To> $| <$2> <>
R<@> <$*> $| <$*>       $: <$2> <$1>            reverse result
R<?> <$*>               $: @ $1         mark address as no match
R<$={Accept}> <$*>      $: @ $2         mark address as no match
R<REJECT> $*                    $#error $@ 5.2.1 $: "550 Mailbox disabled for this recipient"
```

```
R<DISCARD> $*                   $#discard $: discard
R<QUARANTINE:$+> $*             $#error $@ quarantine $: $1
R<ERROR:$-.$-.$-:$+> $*                 $#error $@ $1.$2.$3 $: $4
R<ERROR:$+> $*                  $#error $: $1
R<<TMPF>> $*                    $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again
later."
R<$+> $*            $#error $: $1           error from access db
R@ $*               $1              remove mark
# authenticated via TLS?
R$*                 $: $1 $| $>RelayTLS     client authenticated?
R$* $| $# $+        $# $2                   error/ok?
R$* $| $*           $: $1                   no
R$*                 $: $1 $| $>"Local_Relay_Auth" $&{auth_type}
R$* $| $# $*        $# $2
R$* $| NO           $: $1
R$* $| $*           $: $1 $| $&{auth_type}
R$* $|              $: $1
R$* $| $={TrustAuthMech}    $# RELAY
R$* $| $*           $: $1
# anything terminating locally is ok
R$+ < @ $=w >               $@ RELAY
R$+ < @ $* $=R >    $@ RELAY
R$+ < @ $+ >        $: $>D <$2> <?> <+ To> <$1 < @ $2 >>
R<RELAY> $*         $@ RELAY
R<$* <TMPF>> $*             $#TEMP $@ 4.3.0 $: "451 Temporary system failure. Please try again
later."
R<$*> <$*>          $: $2
# check for local user (i.e. unqualified address)
```

```
R$*                     $: <?> $1
R<?> $* < @ $+ >        $: <REMOTE> $1 < @ $2 >
# local user is ok
R<?> $+                         $@ RELAY
R<$+> $*                $: $2
##########################################################################
### Relay_ok: is the relay/sender ok?
##########################################################################
SRelay_ok
# anything originating locally is ok
# check IP address
R$*                     $: $&{client_addr}
R$@                     $@ RELAY                originated locally
R0                      $@ RELAY                originated locally
R127.0.0.1              $@ RELAY                originated locally
RIPv6:::1               $@ RELAY                originated locally
R$=R $*                         $@ RELAY                relayable IP address
R$*                     $: $>A <$1> <?> <+ Connect> <$1>
R<RELAY> $*                     $@ RELAY                relayable IP address
R<<TMPF>> $*                    $#TEMP $@ 4.3.0 $: "451 Temporary system failure. Please try again
later."
R<$*> <$*>              $: $2
R$*                     $: [ $1 ]               put brackets around it...
R$=w                    $@ RELAY                ... and see if it is local
# check client name: first: did it resolve?
R$*                     $: < $&{client_resolve} >
R<TEMP>                         $#TEMP $@ 4.4.0 $: "450 Relaying temporarily denied. Cannot re-
solve PTR record for " $&{client_addr}
```

```
R<FORGED>           $#error $@ 5.7.1 $: "550 Relaying denied. IP name possibly forged "
$&{client_name}

R<FAIL>                     $#error $@ 5.7.1 $: "550 Relaying denied. IP name lookup failed "
$&{client_name}

R$*                 $: <@> $&{client_name}

# pass to name server to make hostname canonical

R<@> $* $=P         $:<?>  $1 $2

R<@> $+                     $:<?>  $[ $1 $]

R$* .               $1                  strip trailing dots

R<?> $=w            $@ RELAY

R<?> $* $=R                 $@ RELAY

R<?> $*                     $: $>D <$1> <?> <+ Connect> <$1>

R<RELAY> $*         $@ RELAY

R<$* <TMPF>> $*             $#TEMP $@ 4.3.0 $: "451 Temporary system failure. Please try again
later."

R<$*> <$*>          $: $2

##########################################################################

###  F: LookUpFull -- search for an entry in access database

###

###     lookup of full key (which should be an address) and

###     variations if +detail exists: +* and without +detail

###

###     Parameters:

###             <$1> -- key

###             <$2> -- default (what to return if not found in db)

###             <$3> -- mark (must be <(!|+) single-token>)

###                     ! does lookup only with tag

###                     + does lookup with and without tag

###             <$4> -- passthru (additional data passed unchanged through)
```

```
##########################################################################
SF
R<$+> <$*> <$- $-> <$*>                 $: <$(access $4:$1 $: ? $)> <$1> <$2> <$3 $4> <$5>
R<?> <$+> <$*> <+ $-> <$*>  $: <$(access $1 $: ? $)> <$1> <$2> <+ $3> <$4>
R<?> <$+ + $* @ $+> <$*> <$- $-> <$*>
                        $: <$(access $6:$1+*@$3 $: ? $)> <$1+$2@$3> <$4> <$5 $6> <$7>
R<?> <$+ + $* @ $+> <$*> <+ $-> <$*>
                        $: <$(access $1+*@$3 $: ? $)> <$1+$2@$3> <$4> <+ $5> <$6>
R<?> <$+ + $* @ $+> <$*> <$- $-> <$*>
                        $: <$(access $6:$1@$3 $: ? $)> <$1+$2@$3> <$4> <$5 $6> <$7>
R<?> <$+ + $* @ $+> <$*> <+ $-> <$*>
                        $: <$(access $1@$3 $: ? $)> <$1+$2@$3> <$4> <+ $5> <$6>
R<?> <$+> <$*> <$- $-> <$*> $@ <$2> <$5>
R<$+ <TMPF>> <$*> <$- $-> <$*>     $@ <<TMPF>> <$5>
R<$+> <$*> <$- $-> <$*>                 $@ <$1> <$5>
##########################################################################
###  E: LookUpExact -- search for an entry in access database
###
###      Parameters:
###              <$1> -- key
###              <$2> -- default (what to return if not found in db)
###              <$3> -- mark (must be <(!|+) single-token>)
###                      ! does lookup only with tag
###                      + does lookup with and without tag
###              <$4> -- passthru (additional data passed unchanged through)
```

```
##########################################################################
SE
R<$*> <$*> <$- $-> <$*>                 $: <$(access $4:$1 $: ? $)> <$1> <$2> <$3 $4> <$5>
R<?> <$+> <$*> <+ $-> <$*>  $: <$(access $1 $: ? $)> <$1> <$2> <+ $3> <$4>
R<?> <$+> <$*> <$- $-> <$*> $@ <$2> <$5>
R<$+ <TMPF>> <$*> <$- $-> <$*>     $@ <<TMPF>> <$5>
R<$+> <$*> <$- $-> <$*>                 $@ <$1> <$5>
##########################################################################
###  U: LookUpUser -- search for an entry in access database
###
###       lookup of key (which should be a local part) and
###       variations if +detail exists: +* and without +detail
###
###       Parameters:
###               <$1> -- key (user@)
###               <$2> -- default (what to return if not found in db)
###               <$3> -- mark (must be <(!|+) single-token>)
###                       ! does lookup only with tag
###                       + does lookup with and without tag
###               <$4> -- passthru (additional data passed unchanged through)
##########################################################################
SU
R<$+> <$*> <$- $-> <$*>                 $: <$(access $4:$1 $: ? $)> <$1> <$2> <$3 $4> <$5>
R<?> <$+> <$*> <+ $-> <$*>  $: <$(access $1 $: ? $)> <$1> <$2> <+ $3> <$4>
R<?> <$+ + $* @> <$*> <$- $-> <$*>
                        $: <$(access $5:$1+*@ $: ? $)> <$1+$2@> <$3> <$4 $5> <$6>
R<?> <$+ + $* @> <$*> <+ $-> <$*>
                        $: <$(access $1+*@ $: ? $)> <$1+$2@> <$3> <+ $4> <$5>
```

```
R<?> <$+ + $* @> <$*> <$- $-> <$*>
                        $: <$(access $5:$1@ $: ? $)> <$1+$2@> <$3> <$4 $5> <$6>
R<?> <$+ + $* @> <$*> <+ $-> <$*>
                        $: <$(access $1@ $: ? $)> <$1+$2@> <$3> <+ $4> <$5>
R<?> <$+> <$*> <$- $-> <$*> $@ <$2> <$5>
R<$+ <TMPF>> <$*> <$- $-> <$*>     $@ <<TMPF>> <$5>
R<$+> <$*> <$- $-> <$*>                $@ <$1> <$5>
##########################################################################
###  SearchList: search a list of items in the access map
###      Parameters:
###              <exact tag> $| <mark:address> <mark:address> ... <>
###      where "exact" is either "+" or "!":
###      <+ TAG>         lookup with and w/o tag
###      <! TAG>         lookup with tag
###      possible values for "mark" are:
###              D: recursive host lookup (LookUpDomain)
###              E: exact lookup, no modifications
###              F: full lookup, try user+ext@domain and user@domain
###              U: user lookup, try user+ext and user (input must have trailing @)
###      return: <RHS of lookup> or <?> (not found)
##########################################################################
# class with valid marks for SearchList
C{Src}E F D U
SSearchList
# just call the ruleset with the name of the tag... nice trick...
R<$+> $| <$={Src}:$*> <$*>   $: <$1> $| <$4> $| $>$2 <$3> <?> <$1> <>
R<$+> $| <> $| <?> <>            $@ <?>
R<$+> $| <$+> $| <?> <>                $@ $>SearchList <$1> $| <$2>
```

```
R<$+> $| <$*> $| <$+> <>        $@ <$3>
R<$+> $| <$+>                   $@ <$2>
##########################################################################
###  trust_auth: is user trusted to authenticate as someone else?
###
###       Parameters:
###               $1: AUTH= parameter from MAIL command
##########################################################################
SLocal_trust_auth
Strust_auth
R$*                     $: $&{auth_type} $| $1
# required by RFC 2554 section 4.
R$@ $| $*               $#error $@ 5.7.1 $: "550 not authenticated"
R$* $| $&{auth_authen}                  $@ identical
R$* $| <$&{auth_authen}>        $@ identical
R$* $| $*               $: $1 $| $>"Local_trust_auth" $2
R$* $| $#$*             $#$2
R$*                     $#error $@ 5.7.1 $: "550 " $&{auth_authen} " not allowed to act as "
$&{auth_author}
##########################################################################
###  Relay_Auth: allow relaying based on authentication?
###
###       Parameters:
###               $1: ${auth_type}
##########################################################################
SLocal_Relay_Auth
```

```
##########################################################################
###  srv_features: which features to offer to a client?
###       (done in server)
##########################################################################
Ssrv_features
R$*             $: $>D <$&{client_name}> <?> <! "Srv_Features"> <>
R<?>$*                  $: $>A <$&{client_addr}> <?> <! "Srv_Features"> <>
R<?>$*                  $: <$(access "Srv_Features": $: ? $)>
R<?>$*                  $@ OK
R<$* <TMPF>>$*      $#temp
R<$+>$*                 $# $1
##########################################################################
###  try_tls: try to use STARTTLS?
###       (done in client)
##########################################################################
Stry_tls
R$*             $: $>D <$&{server_name}> <?> <! "Try_TLS"> <>
R<?>$*                  $: $>A <$&{server_addr}> <?> <! "Try_TLS"> <>
R<?>$*                  $: <$(access "Try_TLS": $: ? $)>
R<?>$*                  $@ OK
R<$* <TMPF>>$*      $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again later."
R<NO>$*                 $#error $@ 5.7.1 $: "550 do not try TLS with " $&{server_name} "
["$&{server_addr}"]"
##########################################################################
###  tls_rcpt: is connection with server "good" enough?
###       (done in client, per recipient)
###
###       Parameters:
```

```
###             $1: recipient
#########################################################################
Stls_rcpt
R$*                     $: $(macro {TLS_Name} $@ $&{server_name} $) $1
R$+                     $: <?> $>CanonAddr $1
R<?> $+ < @ $+ . >      <?> $1 <@ $2 >
R<?> $+ < @ $+ >        $: $1 <@ $2 > $| <F:$1@$2> <U:$1@> <D:$2> <E:>
R<?> $+                         $: $1 $| <U:$1@> <E:>
R$* $| $+       $: $1 $| $>SearchList <! "TLS_Rcpt"> $| $2 <>
R$* $| <?>      $@ OK
R$* $| <$* <TMPF>>  $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again later."
R$* $| <$+>     $@ $>"TLS_connection" $&{verify} $| <$2>
#########################################################################
###  tls_client: is connection with client "good" enough?
###      (done in server)
###
###      Parameters:
###             ${verify} $| (MAIL|STARTTLS)
#########################################################################
Stls_client
R$*             $: $(macro {TLS_Name} $@ $&{server_name} $) $1
R$* $| $*       $: $1 $| $>D <$&{client_name}> <?> <! "TLS_Clt"> <>
R$* $| <?>$*    $: $1 $| $>A <$&{client_addr}> <?> <! "TLS_Clt"> <>
R$* $| <?>$*    $: $1 $| <$(access "TLS_Clt": $: ? $)>
R$* $| <$* <TMPF>>  $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again later."
R$*             $@ $>"TLS_connection" $1
#########################################################################
###  tls_server: is connection with server "good" enough?
```

```
###      (done in client)
###
###      Parameter:
###              ${verify}
#########################################################################
Stls_server
R$*              $: $(macro {TLS_Name} $@ $&{server_name} $) $1
R$*              $: $1 $| $>D <$&{server_name}> <?> <! "TLS_Srv"> <>
R$* $| <?>$*     $: $1 $| $>A <$&{server_addr}> <?> <! "TLS_Srv"> <>
R$* $| <?>$*     $: $1 $| <$(access "TLS_Srv": $: ? $)>
R$* $| <$* <TMPF>>   $#error $@ 4.3.0 $: "451 Temporary system failure. Please try again later."
R$*              $@ $>"TLS_connection" $1
#########################################################################
###  TLS_connection: is TLS connection "good" enough?
###
###      Parameters:
###              ${verify} $| <Requirement> [<>]
###              Requirement: RHS from access map, may be ? for none.
#########################################################################
STLS_connection
R$* $| <$*>$*                    $: $1 $| <$2>
# create the appropriate error codes
R$* $| <PERM + $={Tls} $*>   $: $1 $| <503:5.7.0> <$2 $3>
R$* $| <TEMP + $={Tls} $*>   $: $1 $| <403:4.7.0> <$2 $3>
R$* $| <$={Tls} $*>              $: $1 $| <403:4.7.0> <$2 $3>
# deal with TLS handshake failures: abort
RSOFTWARE $| <$-:$+> $*    $#error $@ $2 $: $1 " TLS handshake failed."
RSOFTWARE $| $*              $#error $@ 4.7.0 $: "403 TLS handshake failed."
```

```
# deal with TLS protocol errors: abort
RPROTOCOL $| <$-:$+> $*     $#error $@ $2 $: $1 " STARTTLS failed."
RPROTOCOL $| $*             $#error $@ 4.7.0 $: "403 STARTTLS failed."
R$* $| <$*> <VERIFY>                $: <$2> <VERIFY> <> $1
R$* $| <$*> <VERIFY + $+>   $: <$2> <VERIFY> <$3> $1
R$* $| <$*> <$={Tls}:$->$*  $: <$2> <$3:$4> <> $1
R$* $| <$*> <$={Tls}:$- + $+>$*     $: <$2> <$3:$4> <$5> $1
R$* $| $*                   $@ OK
# authentication required: give appropriate error
# other side did authenticate (via STARTTLS)
R<$*><VERIFY> <> OK         $@ OK
R<$*><VERIFY> <$+> OK       $: <$1> <REQ:0> <$2>
R<$*><VERIFY:$-> <$*> OK $: <$1> <REQ:$2> <$3>
R<$*><ENCR:$-> <$*> $*      $: <$1> <REQ:$2> <$3>
R<$-:$+><VERIFY $*> <$*>  $#error $@ $2 $: $1 " authentication required"
R<$-:$+><VERIFY $*> <$*> FAIL   $#error $@ $2 $: $1 " authentication failed"
R<$-:$+><VERIFY $*> <$*> NO     $#error $@ $2 $: $1 " not authenticated"
R<$-:$+><VERIFY $*> <$*> NOT    $#error $@ $2 $: $1 " no authentication requested"
R<$-:$+><VERIFY $*> <$*> NONE   $#error $@ $2 $: $1 " other side does not support START-
TLS"
R<$-:$+><VERIFY $*> <$*> $+     $#error $@ $2 $: $1 " authentication failure " $4
R<$*><REQ:$-> <$*>          $: <$1> <REQ:$2> <$3> $>max $&{cipher_bits} : $&{auth_ssf}
R<$*><REQ:$-> <$*> $-       $: <$1> <$2:$4> <$3> $(arith l $@ $4 $@ $2 $)
R<$-:$+><$-:$-> <$*> TRUE  $#error $@ $2 $: $1 " encryption too weak " $4 " less than " $3
R<$-:$+><$-:$-> <$*> $*     $: <$1:$2 ++ $5>
R<$-:$+ ++ >                $@ OK
R<$-:$+ ++ $+ >             $: <$1:$2> <$3>
R<$-:$+> < $+ ++ $+ >       <$1:$2> <$3> <$4>
```

```
R<$-:$+> $+                     $@ $>"TLS_req" $3 $| <$1:$2>
##########################################################################
###  TLS_req: check additional TLS requirements
###
###      Parameters: [<list> <of> <req>] $| <$-:$+>
###              $-: SMTP reply code
###              $+: Enhanced Status Code
##########################################################################
STLS_req
R $| $+         $@ OK
R<CN> $* $| <$+>                $: <CN:$&{TLS_Name}> $1 $| <$2>
R<CN:$&{cn_subject}> $* $| <$+>             $@ $>"TLS_req" $1 $| <$2>
R<CN:$+> $* $| <$-:$+>          $#error $@ $4 $: $3 " CN " $&{cn_subject} " does not match " $1
R<CS:$&{cert_subject}> $* $| <$+>   $@ $>"TLS_req" $1 $| <$2>
R<CS:$+> $* $| <$-:$+>          $#error $@ $4 $: $3 " Cert Subject " $&{cert_subject} " does not
match " $1
R<CI:$&{cert_issuer}> $* $| <$+>    $@ $>"TLS_req" $1 $| <$2>
R<CI:$+> $* $| <$-:$+>          $#error $@ $4 $: $3 " Cert Issuer " $&{cert_issuer} " does not match
" $1
ROK                     $@ OK
##########################################################################
###  max: return the maximum of two values separated by :
###
###      Parameters: [$-]:[$-]
##########################################################################
Smax
R:              $: 0
R:$-            $: $1
R$-:            $: $1
```

```
R$-:$-          $: $(arith l $@ $1 $@ $2 $) : $1 : $2
RTRUE:$-:$-     $: $2
R$-:$-:$-       $: $2
##########################################################################
###  RelayTLS: allow relaying based on TLS authentication
###
###      Parameters:
###              none
##########################################################################
SRelayTLS
# authenticated?
R$*                     $: <?> $&{verify}
R<?> OK                         $: OK           authenticated: continue
R<?> $*                         $@ NO           not authenticated
R$*                     $: $&{cert_issuer}
R$+                     $: $(access CERTISSUER:$1 $)
RRELAY                          $# RELAY
RSUBJECT                $: <@> $&{cert_subject}
R<@> $+                         $: <@> $(access CERTSUBJECT:$1 $)
R<@> RELAY              $# RELAY
R$*                     $: NO
##########################################################################
###  authinfo: lookup authinfo in the access map
###
###      Parameters:
###              $1: {server_name}
###              $2: {server_addr}
##########################################################################
```

```
Sauthinfo
R$*             $: $1 $| $>D <$&{server_name}> <?> <! AuthInfo> <>
R$* $| <?>$*    $: $1 $| $>A <$&{server_addr}> <?> <! AuthInfo> <>
R$* $| <?>$*    $: $1 $| <$(access AuthInfo: $: ? $)> <>
R$* $| <?>$*    $@ no                           no authinfo available
R$* $| <$*> <>$# $2
#
##########################################################################
##########################################################################
#####
#####                    MAIL FILTER DEFINITIONS
#####
##########################################################################
##########################################################################
Xavmilter, S=inet:3333@127.0.0.1,F=R,T=S:2m;R:2m;E:10m
#
##########################################################################
##########################################################################
#####
#####                    MAILER DEFINITIONS
#####
##########################################################################
##########################################################################
#####################################
###   SMTP Mailer specification   ###
#####################################
#####  $Id: smtp.m4,v 8.64 2001/04/03 01:52:54 gshapiro Exp $  #####
#
```

```
#  common sender and masquerading recipient rewriting
#
SMasqSMTP
R$* < @ $* > $*              $@ $1 < @ $2 > $3          already fully qualified
R$+                          $@ $1 < @ *LOCAL* >        add local qualification
#
#  convert pseudo-domain addresses to real domain addresses
#
SPseudoToReal
# pass <route-addr>s through
R< @ $+ > $*                 $@ < @ $1 > $2             resolve <route-addr>
# output fake domains as user%fake@relay
# do UUCP heuristics; note that these are shared with UUCP mailers
R$+ < @ $+ .UUCP. >          $: < $2 ! > $1             convert to UUCP form
R$+ < @ $* > $*              $@ $1 < @ $2 > $3          not UUCP form
# leave these in .UUCP form to avoid further tampering
R< $&h ! > $- ! $+           $@ $2 < @ $1 .UUCP. >
R< $&h ! > $-.$+ ! $+        $@ $3 < @ $1.$2 >
R< $&h ! > $+                $@ $1 < @ $&h .UUCP. >
R< $+ ! > $+                 $: $1 ! $2 < @ $Y >        use UUCP_RELAY
R$+ < @ $~[ $* : $+ > $@ $1 < @ $4 >                    strip mailer: part
R$+ < @ >                    $: $1 < @ *LOCAL* >        if no UUCP_RELAY
#
#  envelope sender rewriting
#
SEnvFromSMTP
R$+                          $: $>PseudoToReal $1       sender/recipient common
```

```
R$* :; <@>              $@                      list:; special case
R$*                     $: $>MasqSMTP $1        qualify unqual'ed names
R$+                     $: $>MasqEnv $1                 do masquerading
#
#  envelope recipient rewriting --
#  also header recipient if not masquerading recipients
#
SEnvToSMTP
R$+                     $: $>PseudoToReal $1    sender/recipient common
R$+                     $: $>MasqSMTP $1        qualify unqual'ed names
R$* < @ *LOCAL* > $*        $: $1 < @ $j . > $2
#
#  header sender and masquerading header recipient rewriting
#
SHdrFromSMTP
R$+                     $: $>PseudoToReal $1    sender/recipient common
R:; <@>                         $@                      list:; special case
# do special header rewriting
R$* <@> $*              $@ $1 <@> $2            pass null host through
R< @ $* > $*            $@ < @ $1 > $2                  pass route-addr through
R$*                     $: $>MasqSMTP $1        qualify unqual'ed names
R$+                     $: $>MasqHdr $1                 do masquerading
#
#  relay mailer header masquerading recipient rewriting
#
SMasqRelay
R$+                     $: $>MasqSMTP $1
R$+                     $: $>MasqHdr $1
```

Msmtp, P=[IPC], F=mDFMuX, S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP, E=\r\n, L=990,

T=DNS/RFC822/SMTP,

A=TCP $h

Mesmtp, P=[IPC], F=mDFMuXa, S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP, E=\r\n, L=990,

T=DNS/RFC822/SMTP,

A=TCP $h

Msmtp8, P=[IPC], F=mDFMuX8, S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP, E=\r\n, L=990,

T=DNS/RFC822/SMTP,

A=TCP $h

Mdsmtp, P=[IPC], F=mDFMuXa%, S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP, E=\r\n, L=990,

T=DNS/RFC822/SMTP,

A=TCP $h

Mrelay, P=[IPC], F=mDFMuXa8, S=EnvFromSMTP/HdrFromSMTP, R=MasqSMTP, E=\r\n, L=2040,

T=DNS/RFC822/SMTP,

A=TCP $h

######################*****##############

PROCMAIL Mailer specification

###################*****##################

$Id: procmail.m4,v 8.22 2001/11/12 23:11:34 ca Exp $

Mprocmail, P=/usr/bin/procmail, F=DFMSPhnu9, S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP/HdrFromSMTP,

T=DNS/RFC822/X-Unix,

A=procmail -Y -m $h $f $u

##

Local and Program Mailer specification

##

```
#####  $Id: local.m4,v 8.59 2004/11/23 00:37:25 ca Exp $  #####
#
#  Envelope sender rewriting
#
SEnvFromL
R<@>                    $n                      errors to mailer-daemon
R@ <@ $*>               $n                      temporarily bypass Sun bogosity
R$+                     $: $>AddDomain $1       add local domain if needed
R$*                     $: $>MasqEnv $1                 do masquerading
#
#  Envelope recipient rewriting
#
SEnvToL
R$+ < @ $* >            $: $1                   strip host part
#
#  Header sender rewriting
#
SHdrFromL
R<@>                    $n                      errors to mailer-daemon
R@ <@ $*>               $n                      temporarily bypass Sun bogosity
R$+                     $: $>AddDomain $1       add local domain if needed
R$*                     $: $>MasqHdr $1                 do masquerading
#
#  Header recipient rewriting
#
SHdrToL
R$+                     $: $>AddDomain $1       add local domain if needed
R$* < @ *LOCAL* > $*            $: $1 < @ $j . > $2
```

#

Common code to add local domain name (only if always-add-domain)

#

SAddDomain

R$* < @ $* > $* $@ $1 < @ $2 > $3 already fully qualified

R$+ $@ $1 < @ *LOCAL* > add local qualification

Mlocal, P=/usr/bin/procmail, F=lsDFMAw5:/|@qSPfhn9, S=EnvFromL/HdrFromL, R=EnvToL/HdrToL,

T=DNS/RFC822/X-Unix,

A=procmail -t -Y -a $h -d $u

Mprog, P=/usr/sbin/smrsh, F=lsDFMoqeu9, S=EnvFromL/HdrFromL, R=EnvToL/HdrToL, D=$z:/,

T=X-Unix/X-Unix/X-Unix,

A=smrsh -c $u

8.19 /etc/mail/sendmail.mc

divert(-1)dnl

dnl #

dnl # This is the sendmail macro config file for m4. If you make changes to

dnl # /etc/mail/sendmail.mc, you will need to regenerate the

dnl # /etc/mail/sendmail.cf file by confirming that the sendmail-cf package is

dnl # installed and then performing a

dnl #

dnl # make -C /etc/mail

dnl #

include(`/usr/share/sendmail-cf/m4/cf.m4')dnl

VERSIONID(`setup for linux')dnl

OSTYPE(`linux')dnl

dnl #

dnl # Do not advertize sendmail version.

dnl #

dnl define(`confSMTP_LOGIN_MSG', `$j Sendmail; $b')dnl

dnl #

dnl # default logging level is 9, you might want to set it higher to

dnl # debug the configuration

dnl #

dnl define(`confLOG_LEVEL', `9')dnl

dnl #

dnl # Uncomment and edit the following line if your outgoing mail needs to

dnl # be sent out through an external mail server:

dnl #

dnl define(`SMART_HOST', `smtp.your.provider')dnl

dnl #

define(`confDEF_USER_ID', ``8:12")dnl

dnl define(`confAUTO_REBUILD')dnl

define(`confTO_CONNECT', `1m')dnl

define(`confTRY_NULL_MX_LIST', `True')dnl

define(`confDONT_PROBE_INTERFACES', `True')dnl

define(`PROCMAIL_MAILER_PATH', `/usr/bin/procmail')dnl

define(`ALIAS_FILE', `/etc/aliases')dnl

define(`STATUS_FILE', `/var/log/mail/statistics')dnl

define(`UUCP_MAILER_MAX', `2000000')dnl

define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl

define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl

define(`confAUTH_OPTIONS', `A')dnl

dnl # F�r Sendmail 8.11.x

dnl # INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,F=T,T=S:2m;R:2m;E:10m')

dnl # define(`confINPUT_MAIL_FILTERS', `avmilter,filter2,filter1,filter3')

dnl # F�r Sendmail 8.12.x

INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@127.0.0.1,F=R,T=S:2m;R:2m;E:10m')

dnl #

dnl # The following allows relaying if the user authenticates, and disallows

dnl # plaintext authentication (PLAIN/LOGIN) on non-TLS links

dnl #

dnl define(`confAUTH_OPTIONS', `A p')dnl

dnl #

dnl # PLAIN is the preferred plaintext authentication method and used by

dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs do

dnl # use LOGIN. Other mechanisms should be used if the connection is not

dnl # guaranteed secure.

dnl # Please remember that saslauthd needs to be running for AUTH.

dnl #

dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

dnl define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOG-IN PLAIN')dnl

dnl #

dnl # Rudimentary information on creating certificates for sendmail TLS:

dnl # cd /etc/pki/tls/certs; make sendmail.pem

dnl # Complete usage:

dnl # make -C /etc/pki/tls/certs usage

dnl #

dnl define(`confCACERT_PATH', `/etc/pki/tls/certs')dnl

dnl define(`confCACERT', `/etc/pki/tls/certs/ca-bundle.crt')dnl

dnl define(`confSERVER_CERT', `/etc/pki/tls/certs/sendmail.pem')dnl

```
dnl define(`confSERVER_KEY', `/etc/pki/tls/certs/sendmail.pem')dnl
dnl #
dnl # This allows sendmail to use a keyfile that is shared with OpenLDAP's
dnl # slapd, which requires the file to be readble by group ldap
dnl #
dnl define(`confDONT_BLAME_SENDMAIL', `groupreadablekeyfile')dnl
dnl #
dnl define(`confTO_QUEUEWARN', `4h')dnl
dnl define(`confTO_QUEUERETURN', `5d')dnl
dnl define(`confQUEUE_LA', `12')dnl
dnl define(`confREFUSE_LA', `18')dnl
define(`confTO_IDENT', `0')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa', `dnl')dnl
FEATURE(`smrsh', `/usr/sbin/smrsh')dnl
FEATURE(`mailertable', `hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
dnl #
dnl # The following limits the number of processes sendmail can fork to accept
dnl # incoming messages or process its message queues to 20.) sendmail refuses
dnl # to accept connections once it has reached its quota of child processes.
dnl #
dnl define(`confMAX_DAEMON_CHILDREN', `20')dnl
dnl #
```

dnl # Limits the number of new connections per second. This caps the overhead

dnl # incurred due to forking new sendmail processes. May be useful against

dnl # DoS attacks or barrages of spam. (As mentioned below, a per-IP address

dnl # limit would be useful but is not available as an option at this writing.)

dnl #

dnl define(`confCONNECTION_RATE_THROTTLE', `3')dnl

dnl #

dnl # The -t option will retry delivery if e.g. the user runs over his quota.

dnl #

FEATURE(local_procmail, `', `procmail -t -Y -a $h -d $u')dnl

FEATURE(`access_db', `hash -T<TMPF> -o /etc/mail/access.db')dnl

FEATURE(`blacklist_recipients')dnl

dnl EXPOSED_USER(`root')dnl

dnl #

dnl # For using Cyrus-IMAPd as POP3/IMAP server through LMTP delivery uncomment

dnl # the following 2 definitions and activate below in the MAILER section the

dnl # cyrusv2 mailer.

dnl #

dnl define(`confLOCAL_MAILER', `cyrusv2')dnl

dnl define(`CYRUSV2_MAILER_ARGS', `FILE /var/lib/imap/socket/lmtp')dnl

dnl #

dnl # The following causes sendmail to only listen on the IPv4 loopback address

dnl # 127.0.0.1 and not on any other network devices. Remove the loopback

dnl # address restriction to accept email from the internet or intranet.

dnl #

DAEMON_OPTIONS(`Name=MTA,Port=smtp')

dnl #

dnl # The following causes sendmail to additionally listen to port 587 for

dnl # mail from MUAs that authenticate. Roaming users who can't reach their

dnl # preferred sendmail daemon due to port 25 being blocked or redirected find

dnl # this useful.

dnl #

dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl

dnl #

dnl # The following causes sendmail to additionally listen to port 465, but

dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed

dnl # by STARTTLS is preferred, but roaming clients using Outlook Express can't

dnl # do STARTTLS on ports other than 25. Mozilla Mail can ONLY use STARTTLS

dnl # and doesn't support the deprecated smtps; Evolution <1.1.1 uses smtps

dnl # when SSL is enabled-- STARTTLS support is available in version 1.1.1.

dnl #

dnl # For this to work your OpenSSL certificates must be configured.

dnl #

dnl DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl

dnl #

dnl # The following causes sendmail to additionally listen on the IPv6 loopback

dnl # device. Remove the loopback address restriction listen to the network.

dnl #

dnl dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')dnl

dnl #

dnl # enable both ipv6 and ipv4 in sendmail:

dnl #

dnl DAEMON_OPTIONS(`Name=MTA-v4, Family=inet, Name=MTA-v6, Family=inet6')

dnl #

dnl # We strongly recommend not accepting unresolvable domains if you want to

dnl # protect yourself from spam. However, the laptop and users on computers

dnl # that do not have 24x7 DNS do need this.

dnl #

FEATURE(`accept_unresolvable_domains')dnl

dnl #

dnl FEATURE(`relay_based_on_MX')dnl

dnl #

dnl # Also accept email sent to "localhost.localdomain" as local email.

dnl #

LOCAL_DOMAIN(`localhost.localdomain')dnl

dnl #

dnl # The following example makes mail from this host and any additional

dnl # specified domains appear to be sent from mydomain.com

dnl #

dnl MASQUERADE_AS(`mydomain.com')dnl

MASQUERADE_AS(webserver2012)dnl

dnl #

dnl # masquerade not just the headers, but the envelope as well

dnl #

dnl FEATURE(masquerade_envelope)dnl

dnl FEATURE(masquerade_envelope)dnl

dnl #

dnl # masquerade not just @mydomainalias.com, but @*.mydomainalias.com as well

dnl #

dnl FEATURE(masquerade_entire_domain)dnl

dnl #

dnl MASQUERADE_DOMAIN(localhost)dnl

MASQUERADE_DOMAIN(localhost)dnl

MASQUERADE_DOMAIN(relais.bbs.fh-wilhelmshaven.de)dnl

dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl

MASQUERADE_DOMAIN(localhost.localdomain)dnl

dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl

dnl MASQUERADE_DOMAIN(mydomain.lan)dnl

MAILER(smtp)dnl

MAILER(procmail)dnl

dnl MAILER(cyrusv2)dnl

8.20 /etc/httpd/conf/httpd.conf

#

This is the main Apache server configuration file. It contains the

configuration directives that give the server its instructions.

See <URL:http://httpd.apache.org/docs/2.2/> for detailed information.

In particular, see

<URL:http://httpd.apache.org/docs/2.2/mod/directives.html>

for a discussion of each configuration directive.

#

#

Do NOT simply read the instructions in here without understanding

what they do. They're here only as hints or reminders. If you are unsure

consult the online docs. You have been warned.

#

The configuration directives are grouped into three basic sections:

1. Directives that control the operation of the Apache server process as a

whole (the 'global environment').

2. Directives that define the parameters of the 'main' or 'default' server,

which responds to requests that aren't handled by a virtual host.

```
#     These directives also provide default values for the settings
#     of all virtual hosts.
#  3. Settings for virtual hosts, which allow Web requests to be sent to
#     different IP addresses or hostnames and have them handled by the
#     same Apache server process.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/foo.log"
# with ServerRoot set to "/etc/httpd" will be interpreted by the
# server as "/etc/httpd/logs/foo.log".
#
### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#
#
# Don't give away too much information about all the subcomponents
# we are running.  Comment out this line if you don't mind remote sites
# finding out what major optional modules you are running
ServerTokens OS
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
```

```
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the LockFile documentation
# (available at <URL:http://httpd.apache.org/docs/2.2/mod/mpm_common.html#lockfile>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
ServerRoot "/etc/httpd"
#
# PidFile: The file in which the server should record its process
# identification number when it starts.
#
PidFile run/httpd.pid
#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 120
#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive Off
#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100
```

```
#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 15
##
## Server-Pool Size Regulation (MPM specific)
##
# prefork MPM
# StartServers: number of server processes to start
# MinSpareServers: minimum number of server processes which are kept spare
# MaxSpareServers: maximum number of server processes which are kept spare
# ServerLimit: maximum value for MaxClients for the lifetime of the server
# MaxClients: maximum number of server processes allowed to start
# MaxRequestsPerChild: maximum number of requests a server process serves
<IfModule prefork.c>
StartServers       8
MinSpareServers    5
MaxSpareServers   20
ServerLimit      256
MaxClients       256
MaxRequestsPerChild  4000
</IfModule>
# worker MPM
# StartServers: initial number of server processes to start
# MaxClients: maximum number of simultaneous client connections
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
```

```
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestsPerChild: maximum number of requests a server process serves
<IfModule worker.c>
StartServers         2
MaxClients         150
MinSpareThreads     25
MaxSpareThreads     75
ThreadsPerChild     25
MaxRequestsPerChild  0
</IfModule>
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 80
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
```

```
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_dbm_module modules/mod_authn_dbm.so
LoadModule authn_default_module modules/mod_authn_default.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule authz_owner_module modules/mod_authz_owner.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_dbm_module modules/mod_authz_dbm.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule logio_module modules/mod_logio.so
LoadModule env_module modules/mod_env.so
LoadModule ext_filter_module modules/mod_ext_filter.so
LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule expires_module modules/mod_expires.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule headers_module modules/mod_headers.so
```

LoadModule usertrack_module modules/mod_usertrack.so

LoadModule setenvif_module modules/mod_setenvif.so

LoadModule mime_module modules/mod_mime.so

LoadModule dav_module modules/mod_dav.so

LoadModule status_module modules/mod_status.so

LoadModule autoindex_module modules/mod_autoindex.so

LoadModule info_module modules/mod_info.so

LoadModule dav_fs_module modules/mod_dav_fs.so

LoadModule vhost_alias_module modules/mod_vhost_alias.so

LoadModule negotiation_module modules/mod_negotiation.so

LoadModule dir_module modules/mod_dir.so

LoadModule actions_module modules/mod_actions.so

LoadModule speling_module modules/mod_speling.so

LoadModule userdir_module modules/mod_userdir.so

LoadModule alias_module modules/mod_alias.so

LoadModule rewrite_module modules/mod_rewrite.so

LoadModule proxy_module modules/mod_proxy.so

LoadModule proxy_balancer_module modules/mod_proxy_balancer.so

LoadModule proxy_ftp_module modules/mod_proxy_ftp.so

LoadModule proxy_http_module modules/mod_proxy_http.so

LoadModule proxy_connect_module modules/mod_proxy_connect.so

LoadModule cache_module modules/mod_cache.so

LoadModule suexec_module modules/mod_suexec.so

LoadModule disk_cache_module modules/mod_disk_cache.so

LoadModule file_cache_module modules/mod_file_cache.so

LoadModule mem_cache_module modules/mod_mem_cache.so

LoadModule cgi_module modules/mod_cgi.so

#

```
# The following modules are not loaded by default:
#
#LoadModule cern_meta_module modules/mod_cern_meta.so
#LoadModule asis_module modules/mod_asis.so
#
# Load config files from the config directory "/etc/httpd/conf.d".
#
Include conf.d/*.conf
#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information (ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
#ExtendedStatus On
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
#  . On SCO (ODT 3) use "User nouser" and "Group nogroup".
#  . On HPUX you may not be able to use shared memory as nobody, and the
#    suggested workaround is to create a user www and use that user.
#  NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
#  when the value of (unsigned)Group is above 60000;
#  don't use Group #-1 on these systems!
#
User apache
Group apache
```

Section 2: 'Main' server configuration

#

The directives in this section set up the values used by the 'main'

server, which responds to any requests that aren't handled by a

<VirtualHost> definition. These values also provide defaults for

any <VirtualHost> containers you may define later in the file.

#

All of these directives may appear inside <VirtualHost> containers,

in which case these default settings will be overridden for the

virtual host being defined.

#

#

ServerAdmin: Your address, where problems with the server should be

e-mailed. This address appears on some server-generated pages, such

as error documents. e.g. admin@your-domain.com

#

ServerAdmin root@localhost

#

ServerName gives the name and port that the server uses to identify itself.

This can often be determined automatically, but we recommend you specify

it explicitly to prevent problems during startup.

#

If this is not set to valid DNS name for your host, server-generated

redirections will not work. See also the UseCanonicalName directive.

#

If your host doesn't have a registered DNS name, enter its IP address here.

You will have to access it by its address anyway, and this will make

redirections work in a sensible way.

```
#
#ServerName www.example.com:80
#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.  When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

```
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/var/www/html">
#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important.  Please see
# http://httpd.apache.org/docs/2.2/mod/core.html#options
# for more information.
#
    Options Indexes FollowSymLinks
#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
```

```
    AllowOverride None
#
# Controls who can get stuff from this server.
#
    Order allow,deny
    Allow from all
</Directory>
#
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
# See also: http://httpd.apache.org/docs/misc/FAQ.html#forbidden
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    UserDir disable
    #
    # To enable requests to /~user/ to serve the user's public_html
```

```
    # directory, remove the "UserDir disable" line above, and uncomment
    # the following line instead:
    #
    #UserDir public_html
</IfModule>
#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
#<Directory /home/*/public_html>
#    AllowOverride FileInfo AuthConfig Limit
#    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
#    <Limit GET POST OPTIONS>
#        Order allow,deny
#        Allow from all
#    </Limit>
#    <LimitExcept GET POST OPTIONS>
#        Order deny,allow
#        Deny from all
#    </LimitExcept>
#</Directory>
#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
```

```
#
DirectoryIndex index.html index.html.var
#
# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives.  See also the AllowOverride
# directive.
#
AccessFileName .htaccess
#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>
#
# TypesConfig describes where the mime.types file (or equivalent) is
# to be found.
#
TypesConfig /etc/mime.types
#
# DefaultType is the default MIME type the server will use for a document
# if it cannot otherwise determine one, such as from filename extensions.
# If your server contains mostly text or HTML documents, "text/plain" is
# a good value.  If most of your content is binary, such as applications
# or images, you may want to use "application/octet-stream" instead to
# keep browsers from trying to display binary files as though they are
```

```
# text.
#
DefaultType text/plain
#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type.  The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
<IfModule mod_mime_magic.c>
#   MIMEMagicFile /usr/share/magic.mime
    MIMEMagicFile conf/magic
</IfModule>
#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off
#
# EnableMMAP: Control whether memory-mapping is used to deliver
# files (assuming that the underlying OS supports it).
# The default is on; turn this off if you serve from NFS-mounted
# filesystems.  On some systems, turning it off (regardless of
# filesystem) can improve performance; for details, please see
# http://httpd.apache.org/docs/2.2/mod/core.html#enablemmap
```

```
#
#EnableMMAP off
#
# EnableSendfile: Control whether the sendfile kernel support is
# used to deliver files (assuming that the OS supports it).
# The default is on; turn this off if you serve from NFS-mounted
# filesystems.  Please see
# http://httpd.apache.org/docs/2.2/mod/core.html#enablesendfile
#
#EnableSendfile off
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn
#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
```

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

LogFormat "%{Referer}i -> %U" referer

LogFormat "%{User-agent}i" agent

"combinedio" includes actual counts of actual bytes received (%I) and sent (%O); this

requires the mod_logio module to be loaded.

#LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio

#

The location and format of the access logfile (Common Logfile Format).

If you do not define any access logfiles within a <VirtualHost>

container, they will be logged here. Contrariwise, if you *do*

define per-<VirtualHost> access logfiles, transactions will be

logged therein and *not* in this file.

#

#CustomLog logs/access_log common

#

If you would like to have separate agent and referer logfiles, uncomment

the following directives.

#

#CustomLog logs/referer_log referer

#CustomLog logs/agent_log agent

#

For a single logfile with access, agent, and referer information

(Combined Logfile Format), use the following directive:

#

CustomLog logs/access_log combined

#

```
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature On
#
# Aliases: Add here as many aliases as you need (with no limit). The format is
# Alias fakename realname
#
# Note that if you include a trailing / on fakename then the server will
# require it to be present in the URL.  So "/icons" isn't aliased in this
# example, only "/icons/".  If the fakename is slash-terminated, then the
# realname must also be slash terminated, and if the fakename omits the
# trailing slash, the realname must also omit it.
#
# We include the /icons/ alias for FancyIndexed directory listings.  If you
# do not use FancyIndexing, you may comment this out.
#
Alias /icons/ "/var/www/icons/"
<Directory "/var/www/icons">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

```
#
# WebDAV module configuration section.
#
<IfModule mod_dav_fs.c>
    # Location of the WebDAV lock database.
    DAVLockDB /var/lib/dav/lockdb
</IfModule>
#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the realname directory are treated as applications and
# run by the server when requested rather than as documents sent to the client.
# The same rules about trailing "/" apply to ScriptAlias directives as to
# Alias.
#
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
#
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
#
# Redirect allows you to tell clients about documents which used to exist in
```

```
# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Example:
# Redirect permanent /foo http://www.example.com/bar
#
# Directives controlling the display of server-generated directory listings.
#
#
# IndexOptions: Controls the appearance of server-generated directory
# listings.
#
IndexOptions FancyIndexing VersionSort NameWidth=* HTMLTable
#
# AddIcon* directives tell the server which icon to show for different
# files or filename extensions.  These are only displayed for
# FancyIndexed directories.
#
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*
AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
```

AddIcon /icons/layout.gif .html .shtml .htm .pdf

AddIcon /icons/text.gif .txt

AddIcon /icons/c.gif .c

AddIcon /icons/p.gif .pl .py

AddIcon /icons/f.gif .for

AddIcon /icons/dvi.gif .dvi

AddIcon /icons/uuencoded.gif .uu

AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl

AddIcon /icons/tex.gif .tex

AddIcon /icons/bomb.gif core

AddIcon /icons/back.gif ..

AddIcon /icons/hand.right.gif README

AddIcon /icons/folder.gif ^^DIRECTORY^^

AddIcon /icons/blank.gif ^^BLANKICON^^

#

DefaultIcon is which icon to show for files which do not have an icon

explicitly set.

#

DefaultIcon /icons/unknown.gif

#

AddDescription allows you to place a short description after a file in

server-generated indexes. These are only displayed for FancyIndexed

directories.

Format: AddDescription "description" filename

#

#AddDescription "GZIP compressed document" .gz

#AddDescription "tar archive" .tar

#AddDescription "GZIP compressed tar archive" .tgz

```
#
# ReadmeName is the name of the README file the server will look for by
# default, and append to directory listings.
#
# HeaderName is the name of a file which should be prepended to
# directory indexes.
ReadmeName README.html
HeaderName HEADER.html
#
# IndexIgnore is a set of filenames which directory indexing should ignore
# and not include in the listing.  Shell-style wildcarding is permitted.
#
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
#
# DefaultLanguage and AddLanguage allows you to specify the language of
# a document. You can then use content negotiation to give a browser a
# file in a language the user can understand.
#
# Specify a default language. This means that all data
# going out without a specific language tag (see below) will
# be marked with this one. You probably do NOT want to set
# this unless you are sure it is correct for all cases.
#
# * It is generally better to not mark a page as
# * being a certain language than marking it with the wrong
# * language!
#
# DefaultLanguage nl
```

```
#
# Note 1: The suffix does not have to be the same as the language
# keyword --- those with documents in Polish (whose net-standard
# language code is pl) may wish to use "AddLanguage pl .po" to
# avoid the ambiguity with the common suffix for perl scripts.
#
# Note 2: The example entries below illustrate that in some cases
# the two character 'Language' abbreviation is not identical to
# the two character 'Country' code for its country,
# E.g. 'Danmark/dk' versus 'Danish/da'.
#
# Note 3: In the case of 'ltz' we violate the RFC by using a three char
# specifier. There is 'work in progress' to fix this and get
# the reference data for rfc1766 cleaned up.
#
# Catalan (ca) - Croatian (hr) - Czech (cs) - Danish (da) - Dutch (nl)
# English (en) - Esperanto (eo) - Estonian (et) - French (fr) - German (de)
# Greek-Modern (el) - Hebrew (he) - Italian (it) - Japanese (ja)
# Korean (ko) - Luxembourgeois* (ltz) - Norwegian Nynorsk (nn)
# Norwegian (no) - Polish (pl) - Portugese (pt)
# Brazilian Portuguese (pt-BR) - Russian (ru) - Swedish (sv)
# Simplified Chinese (zh-CN) - Spanish (es) - Traditional Chinese (zh-TW)
#
AddLanguage ca .ca
AddLanguage cs .cz .cs
AddLanguage da .dk
AddLanguage de .de
AddLanguage el .el
```

AddLanguage en .en

AddLanguage eo .eo

AddLanguage es .es

AddLanguage et .et

AddLanguage fr .fr

AddLanguage he .he

AddLanguage hr .hr

AddLanguage it .it

AddLanguage ja .ja

AddLanguage ko .ko

AddLanguage ltz .ltz

AddLanguage nl .nl

AddLanguage nn .nn

AddLanguage no .no

AddLanguage pl .po

AddLanguage pt .pt

AddLanguage pt-BR .pt-br

AddLanguage ru .ru

AddLanguage sv .sv

AddLanguage zh-CN .zh-cn

AddLanguage zh-TW .zh-tw

#

LanguagePriority allows you to give precedence to some languages

in case of a tie during content negotiation.

#

Just list the languages in decreasing order of preference. We have

more or less alphabetized them here. You probably want to change this.

#

LanguagePriority en ca cs da de el eo es et fr he hr it ja ko ltz nl nn no pl pt pt-BR ru sv zh-CN zh-TW

#

ForceLanguagePriority allows you to serve a result page rather than

MULTIPLE CHOICES (Prefer) [in case of a tie] or NOT ACCEPTABLE (Fallback)

[in case no accepted languages matched the available variants]

#

ForceLanguagePriority Prefer Fallback

#

Specify a default charset for all content served; this enables

interpretation of all content as UTF-8 by default. To use the

default browser choice (ISO-8859-1), or to allow the META tags

in HTML content to override this choice, comment out this

directive:

#

AddDefaultCharset UTF-8

AddDefaultCharset ISO-8859-1

#

AddType allows you to add to or override the MIME configuration

file mime.types for specific file types.

#

#AddType application/x-tar .tgz

#

AddEncoding allows you to have certain browsers uncompress

information on the fly. Note: Not all browsers support this.

Despite the name similarity, the following Add* directives have nothing

to do with the FancyIndexing customization directives above.

#

#AddEncoding x-compress .Z

```
#AddEncoding x-gzip .gz .tgz
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
#
# AddHandler allows you to map certain file extensions to "handlers":
# actions unrelated to filetype. These can be either built into the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options" directive.)
#
#AddHandler cgi-script .cgi
#
# For files that include their own HTTP headers:
#
#AddHandler send-as-is asis
#
# For type maps (negotiated resources):
# (This is enabled by default to allow the Apache "It Worked" page
#  to be distributed in multiple languages.)
#
AddHandler type-map var
#
# Filters allow you to process content before it is sent to the client.
#
```

To parse .shtml files for server-side includes (SSI):

(You will also need to add "Includes" to the "Options" directive.)

#

AddType text/html .shtml

AddOutputFilter INCLUDES .shtml

#

Action lets you define media types that will execute a script whenever

a matching file is called. This eliminates the need for repeated URL

pathnames for oft-used CGI file processors.

Format: Action media/type /cgi-script/location

Format: Action handler-name /cgi-script/location

#

#

Customizable error responses come in three flavors:

1) plain text 2) local redirects 3) external redirects

#

Some examples:

#ErrorDocument 500 "The server made a boo boo."

#ErrorDocument 404 /missing.html

#ErrorDocument 404 "/cgi-bin/missing_handler.pl"

#ErrorDocument 402 http://www.example.com/subscription_info.html

#

#

Putting this all together, we can internationalize error responses.

#

We use Alias to redirect any /error/HTTP_<error>.html.var response to

our collection of by-error message multi-language collections. We use

includes to substitute the appropriate text.

```
#
# You can modify the messages' appearance without changing any of the
# default HTTP_<error>.html.var files by adding the line:
#
#   Alias /error/include/ "/your/include/path/"
#
# which allows you to create your own set of files by starting with the
# /var/www/error/include/ files and
# copying them to /your/include/path/, even on a per-VirtualHost basis.
#
Alias /error/ "/var/www/error/"
<IfModule mod_negotiation.c>
<IfModule mod_include.c>
    <Directory "/var/www/error">
        AllowOverride None
        Options IncludesNoExec
        AddOutputFilter Includes html
        AddHandler type-map var
        Order allow,deny
        Allow from all
        LanguagePriority en es de fr
        ForceLanguagePriority Prefer Fallback
       </Directory>
#    ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
#    ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
#    ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
#    ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
#    ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
```

```
#    ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
#    ErrorDocument 410 /error/HTTP_GONE.html.var
#    ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
#    ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
#    ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
#    ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
#    ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
#    ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
#    ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
#    ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
#    ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
#    ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var
</IfModule>
</IfModule>
#
# The following directives modify normal HTTP response behavior to
# handle known problems with browser implementations.
#
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
#
# The following directive disables redirects on non-GET requests for
# a directory that does not include the trailing slash.  This fixes a
# problem with Microsoft WebFolders which does not appropriately handle
# redirects for folders with DAV methods.
```

```
# Same deal with Apple's DAV filesystem and Gnome VFS support for DAV.
#
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
#
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
# Change the ".example.com" to match your domain to enable.
#
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .example.com
#</Location>
#
# Allow remote server configuration reports, with the URL of
#  http://servername/server-info (requires that mod_info.c be loaded).
# Change the ".example.com" to match your domain to enable.
#
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
```

```
#    Deny from all
#    Allow from .example.com
#</Location>
#
# Proxy Server directives. Uncomment the following lines to
# enable the proxy server:
#
#<IfModule mod_proxy.c>
#ProxyRequests On
#
#<Proxy *>
#    Order deny,allow
#    Deny from all
#    Allow from .example.com
#</Proxy>
#
# Enable/disable the handling of HTTP/1.1 "Via:" headers.
# ("Full" adds the server version; "Block" removes all outgoing Via: headers)
# Set to one of: Off | On | Full | Block
#
#ProxyVia On
#
# To enable a cache of proxied content, uncomment the following lines.
# See http://httpd.apache.org/docs/2.2/mod/mod_cache.html for more details.
#
#<IfModule mod_disk_cache.c>
#   CacheEnable disk /
#   CacheRoot "/var/cache/mod_proxy"
```

```
#</IfModule>
#
#</IfModule>
# End of proxy directives.
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
#
# Use name-based virtual hosting.
#
#NameVirtualHost *:80
#
# NOTE: NameVirtualHost cannot be used without a port specifier
# (e.g. :80) if mod_ssl is being used, due to the nature of the
# SSL protocol.
#
#
# VirtualHost example:
```

```
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without a known
# server name.
#
#<VirtualHost *:80>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
######   www.bbs.fh-wilhelmshaven.de in /etc/hosts eintragen !!!
### ########################################
NameVirtualHost localhost:80
<VirtualHost localhost:80>
ServerName localhost
</VirtualHost>
NameVirtualHost www.bbs.fh-wilhelmshaven.de:80
<VirtualHost www.bbs.fh-wilhelmshaven.de:80>
ServerName www.bbs.fh-wilhelmshaven.de
RewriteEngine On
RewriteRule ^/$ bbsfhome/ [R]
## Nur, wenn Zugrif direkt auf Zope von aussen gewuenscht !!!
#RewriteCond  %{REQUEST_URI} ^/manage
#RewriteRule ^/(.*) http://127.0.0.1:8080/VirtualHostBase/http/www.bbs.fh-
wilhelmshaven.de:80///VirtualHostRoot/$1 [L,P]
## Fuer Verzeichnis mit statischen Websides
#RewriteCond  %{REQUEST_URI} !^/statisch
```

#RewriteCond %{REQUEST_URI} !^/stundenplan

Fuer Portal (Projekte)

RewriteCond %{REQUEST_URI} !^/portal

Fuer Wetter update

#RewriteCond %{REQUEST_URI} !^/wetter

Fuer Bistro

#RewriteCond %{REQUEST_URI} !^/bistro

Fuer Infothek

#RewriteCond %{REQUEST_URI} !^/infothek

Fuer Quickinfo

#RewriteCond %{REQUEST_URI} !^/quickinfo

Fuer phprojekt update

#RewriteCond %{REQUEST_URI} !^/gware

Fuer neue BBSF-Seite mit typo3

#RewriteCond %{REQUEST_URI} !^/bbsfhome

Fuer ZMS

#RewriteRule ^/(.*) http://127.0.0.1:8080/VirtualHostBase/http/www.bbs.fh-wilhelmshaven.de:80/BBSFriedenstr/VirtualHostRoot/$1 [L,P]

</VirtualHost>

<Directory "/var/www/html/portal/mysqldumper">

AuthType Basic

AllowOverride AuthConfig

</Directory>

<Directory "/var/www/html/portal">

AddDefaultCharset ISO-8859-1

LanguagePriority

</Directory>

8.21 /etc/my.cnf

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
# To enable the InnoDB Plugin, uncomment the 2 next lines
#ignore-builtin-innodb
#plugin-load=innodb=ha_innodb_plugin.so
# To enable InnoDB-related INFORMATION_SCHEMA tables
# Join the following options to above directive
  ;innodb_trx=ha_innodb_plugin.so
  ;innodb_locks=ha_innodb_plugin.so
  ;innodb_cmp=ha_innodb_plugin.so
  ;innodb_cmp_reset=ha_innodb_plugin.so
  ;innodb_cmpmem=ha_innodb_plugin.so
  ;innodb_cmpmem_reset=ha_innodb_plugin.so
[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

8.22 /etc/ntp.conf

```
# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

```
# Permit all access over the loopback interface.  This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1
# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
server de.pool.ntp.org
#broadcast 192.168.1.255 key 42                 # broadcast server
#broadcastclient                        # broadcast client
#broadcast 224.0.1.1 key 42             # multicast server
#multicastclient 224.0.1.1              # multicast client
#manycastserver 239.255.254.254                 # manycast server
#manycastclient 239.255.254.254 key 42          # manycast client
# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available.
server   127.127.1.0      # local clock
fudge    127.127.1.0 stratum 10
# Drift file.  Put this in a directory which the daemon can write to.
# No symbolic links allowed, either, since the daemon updates the file
# by creating a temporary in the same directory and then rename()'ing
# it to the file.
driftfile /var/lib/ntp/drift
```

Key file containing the keys and key identifiers used when operating

with symmetric key cryptography.

keys /etc/ntp/keys

Specify the key identifiers which are trusted.

#trustedkey 4 8 42

Specify the key identifier to use with the ntpdc utility.

#requestkey 8

Specify the key identifier to use with the ntpq utility.

#controlkey 8